



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

경영학 박사학위논문

Two Essays on User Behaviors in Online Games

온라인 게임에서 유저의 행태에 관한 연구

2018년 2월

서울대학교 대학원

경영학과 경영학 전공

안 대 환

Two Essays on User Behaviors in Online Games

지도교수 유 병 준

이 논문을 경영학 박사학위논문으로 제출함

2018년 2월

서울대학교 대학원

경영학과 경영정보 전공

안 대 환

안대환의 박사학위논문을 인준함

2018년 2월

위 원 장 _____ (인)

부위원장 _____ (인)

위 원 _____ (인)

위 원 _____ (인)

위 원 _____ (인)

ABSTRACT

Two Essays on User Behaviors in Online Games

Daehwan Ahn

Business School

Seoul National University

This dissertation consists of two essays on user behavior in online games.

In the first essay, I identified multi-botting cheaters and measured their impacts using basic information in database such as user ID, playtime and item purchase record. I addressed the data availability issue and proposed a method for companies with limited data and resources. I also avoided large-scale transaction processing or complex development, which are fairly common in existing cheating detection methods. With respect to identifying cheaters, we used algorithms named DTW (Dynamic Time Warping) and JWD (Jaro–Winkler distance). I also measured the effects of using hacking tool by employing DID (Difference in Differences). My analysis results show some counter-intuitive results. Overall, cheaters constitute a minute part of users in terms of numbers – only about 0.25%. However, they hold approximately 12% of revenue. Furthermore, the usage of hacking tools causes a 102% and 79% increase in playtime and purchase respectively right after users start to use hacking tools. According to additional analysis, it could be shown that the positive effects of hacking tools are not just short-term. My granger causality test also reveals that cheating users' activity does not affect other users' purchases or

playtime trend.

In the second essay, I propose a methodology to deal with churn prediction that meets two major purposes in the mobile casual game context. First, reducing the cost of data preparation, which is growing its importance in the big-data environment. Second, coming up with an algorithm that shows favorable performance comparable to that of the state-of-the-art. As a result, we succeed in greatly lowering the cost of the data preparation process by employing the sequence structure of the log data as it is. In addition, our sequence classification model based on CNN-LSTM shows superior results compared to the models of previous studies.

Keywords: online game, mobile game, cheating, churn, data analysis

Student Number: 2014-30155

TABLE OF CONTENTS

Essay 1. Is Cheating Always Bad? A study of cheating identification and measurement of the effect

1. Introduction
2. Literature Review
3. Data
4. Hypotheses
5. Methodology
 - 5.1 Cheating Identification
 - 5.2 Measurement of Cheating Tool Usage Effect
6. Result
 - 6.1 Cheating Identification
 - 6.2 Measurement of Cheating Tool Usage Effect
7. Additional Analysis
 - 7.1 Lifespan of Cheating Users
 - 7.2 Granger Causality Test
8. Discussion and Conclusion
9. References

Essay 2. Churn Prediction in Mobile Casual Game: A Deep Sequence Classification Approach

1. Introduction
2. Definition of Churn
3. Related Works
4. Data
5. Methodology
 - 5.1 Data Preparation
 - 5.2 Prediction Model
6. Result and Discussion
7. References

Essay 1

Is Cheating Always Bad?

A study of cheating identification and
measurement of the effect

1. Introduction

In real-life business cases, making a right decision is extremely difficult because our common sense does not necessarily lead to good results. Research on such counterintuitive results can easily be seen in the IS research field, especially in the security field. For example, August and Tunca (2008) find out that software vendors should allow users of unlicensed (pirated) copies of a software product to apply security patches because by doing so they can maximize the firm's profits in certain situations. Arora et al. (2008) explain optimal policy for software vulnerability disclosure, arguing that the vendor should release the patch after a certain time period, rather than instantly disclosing it. Therefore, in order to make a right decision, it is quintessential to predict the impact of decision maker's choice correctly.

This study is about a problem of cheating that a Korean game provider faces. The game provider of interest has provided MMORPG service for ten years. The game users grow their avatar and gain cyber money needed for game playing by performing time-consuming activities, such as engaging in battles against monsters. If the player purchases cash items in games by spending fiat currency, he or she is able to save time by making his or her avatar grow quickly with less effort. Basically, players can enjoy the game for free but the provider earns profit by selling such "cash items" to users who are willing take an advantageous position by spending money (Free to Play).

One of the problems the provider faces is that the revenue of the game has decreased over the last two years. They conjecture that one of the reasons for such

trend might be the existence of “cheaters.” However, they are not certain that “cheaters” play a crucial role in damaging the revenue of the firm. Here, “cheating” refers to the activity of logging into several IDs at the same time by one user (Multiboxing), and automatizing the process of making their avatars go for battles by using hacking tools called “bots.” Generally, in order to make their avatars grow stronger, players need to engage in battles, spending their own time or buying cash items. However, if one cheats, they can make their avatars grow consistently even when the he or she is not paying attention. Consequently, when cheating, it would be fairly unnecessary for the player to buy cash items to make their avatar become stronger quickly

Even though the provider is well aware of the existence of cheaters, they are having a hard time making decision whether they should ban the cheaters. The reasons are: 1) they cannot confidently identify who the cheaters are, and 2) they are uncertain whether the existence of the cheaters actually have a negative influence on the revenues.

The problem of deciding who cheaters are and whether to kick them out is not as simple as it seems. To start with, categorizing the behavior of cheating as simply detrimental or evil is rather problematic; cheating is a complicated behavior with a number of pros and cons. That is why there has been much ongoing controversy regarding cheating in the video games (Consalvo, 2009).

Cheating can be defined as the act of destroying the rules of the game that everyone has to obey, as predetermined by the developer. Cheating in online games has a negative impact on users who invested time, money and emotional

attachment to raise their avatars (Aboukhadijeh, 2009). In other words, cheating behavior can negatively influence users that do not cheat by making them feel unjust or unfair. According to Adams (1963), people compare their inputs and outputs to those of others in organizations when determining “equity.” As cheaters outperform non-cheaters with relatively tiny amount of inputs, non-cheaters are prone to feel deprived and undeserved. Such “relative deprivation” that leads to perceived injustice; it should be noted that “deprivation is perceived relationally.” To put it more measurably, two people, hypothetically A and B, tend to assume that “distributive justice” is achieved when:

$$\frac{A's\ rewards - A's\ costs}{A's\ investments} = \frac{B's\ rewards - B's\ costs}{B's\ investment}$$

Hence, under the existence of cheaters, most non-cheaters are likely to perceive “relative deprivation,” leading to distributive injustice among users in gaming community (Adams 1965).

In addition, multiboxing and bots accelerate content consumption and increase server operating costs. As cheaters play games with multiple IDs without intermission, they incur great costs to the provider. To make matters worse, such problem can be further exacerbated by ongoing arms race between users (Taylor, 2009). As people feel that they are outrun by being “cheated” by other players, they are likely to pull another trigger by engaging in additional cheating behaviors. In fact, in order to outrun others, they would have to “cheat” more craftily and intensively, significantly increasing the burden of operating costs for the provider.

With “the Red Queen effect” plaguing users (Ridley 1994), some users might drop out of the game due to the fatigue of ever-increasing competition, or some can continually engage in ever-expanding arms race of cheating.

However, despite such obvious negative effects, cheating can sometimes turn out to be beneficial for both users and the provider. Cheating can enhance gaming experience for users in games that are not perfectly designed. For example, when users are stuck or get bored with games, cheating can help the user to find the new joy of the game again by overcoming the situation and jumping into an interesting part (Consalvo 2009). Cheating can also give users new fun by creating creative rules that game developers did not expect at the outset (Green and Kaufman, 2015).

In a sense, cheating behaviors can be seen as an instance of “the invisible hands” (Smith, 1827). Cheating can be deemed as self-coping mechanisms to complement and circumvent the “rules of the game,” which are somewhat incomplete and unrealistic. The players merely act out of their self-interests, while benefiting the whole. In such cases, game providers can enhance user experience and customer loyalty by subscribing to the gospel of *laissez faire*, allowing people to cheat and compete among themselves.

In addition, to overcome the imperfections and absurdities of the gaming environment, users collectively gather their intelligence, consummating the “wisdom of crowds.” Sometimes, users create or discover new rules and elements, diversifying the contents of the game and elongating the lifespan of the game. For instance, users succeed in generating whole new contents, such as a mod (short for “modification”). A mod is an alteration that modifies some aspect of a game, such

as how it behaves or looks. Mods may reach from small modifications to complete overhauls, and they can enhance the value and interest of the game (Mod (video gaming), n.d.).

In the end, in order to decide whether or not to ban the cheating users, it should be preceded by a careful and thorough analysis of how many there are, how they behave, and how they affect the game, based on real-world data. However, cheating is hard to measure, although it repeatedly occurs in most multiplayer online games (Pritchard, 2000). In many cases, it is difficult to conduct data analysis using game data since the data are not stored systematically and organically. In general, game companies tend to design their database not for efficient data analyses, but for the optimized operation of game. Hence, extracting the data necessary for analysis is highly costly and troublesome for the gaming industry. Moreover, unlike the case of detecting churn, it is relatively difficult to come up with a cheating identification model as there are scarce pre-labeled data regarding who are the cheaters. Unfortunately, our case is not an exception. Because of the data availability issue, it is important to conduct data analysis using limited data sets such as in our study.

In this study, I identified multi-botting cheaters and measured their impacts using basic information in database such as user ID, playtime and item purchase record. I addressed the data availability issue and proposed a method for companies with limited data and resources. I also avoided large-scale transaction processing or complex development, which are fairly common in existing cheating detection methods. With respect to identifying cheaters, I used algorithms named DTW (Dynamic Time Warping) and JWD (Jaro–Winkler distance). I also measured the effects of using hacking tool by employing DID (Difference in Differences).

Our analysis results show some counter-intuitive results. Overall, cheaters constitute a minute part of users in terms of numbers – only about 0.25%. However, they hold approximately 12% of revenue. Furthermore, the usage of hacking tools causes a 102% and 79% increase in playtime and purchase respectively right after users start to use hacking tools. According to additional analysis, it could be shown that the positive effects of hacking tools are not just short-term. Our granger causality test also reveals that cheating users' activity does not affect other users' purchases or playtime trend.

Despite our results showing that cheating has a rather positive side, I was not fully convinced that it is just to allow cheating. I thought that the result of granger causality test could be generalized only in some specific situations. I suspected that cheating users do not have a significant effect on other users because the number of cheating users is too small. I could not predict how they would affect other users if the number of cheaters increases. Many existing studies also warn these side effects of cheating in online games (Thawonmas et al., 2008; Gianvecchio et al., 2009; Yan and Randell, 2009; Kang et al., 2013).

Nevertheless, I was not also entirely in favor of a policy to ban cheating right away. I have already found that a small number of cheating users account for 12% of sales. For the interest of the provider, it is not easy to make a decision to kick users with grave importance. In the end, I came up with alternatives to solve this problem, while minimizing the risk of losing loyal users.

To solve the problem of cheating, I decided to focus on the reason why users cheat. To this end, I closely observe the behaviors of the 207 users that I identified as

cheaters and refer to Consalvo (2006)'s study of why cheating occurs in the game. As a result, it was concluded that the cheating was caused by the game design that forces the users to repeatedly spend time for the growth of the avatar. The game on this paper is approximately 10 years ago, so it was rather afar from the recent game trends that emphasize speed and variety of enjoyment. Cheating users were bored with the characteristics of the game and wanted to reduce tedious repetitions through cheating. Based on these conclusions, I advised that the direction of the new update should focus on reducing the advantage of cheating and increasing the speed of the game and the variety of the contents. As a result, after the new update reflecting our advice, the firm's revenue was able to turn upward once again.

2. Literature Review

With respect to cheating behavior in online games, many existing studies try to examine the taxonomies of cheating behaviors. This is mainly because there does not exist single definition that is generally accepted as game providers beg to differ regarding the criteria used to determine whether a certain behavior is cheating or not (Duh & Chen, 2009). According to Yan (2003), this lack of consistency is due to: 1) cheating in online games is a relatively newborn topic for researchers, 2) wide variety of online game genres leads to different types of cheating, and 3) newer cheating methods are constantly invented as the providers block the existing cheating methods. For such reasons, a number of prior studies aim to focus on defining and classifying various cheating behaviors with a specific set of criteria (Yan & Randell, 2005; Duh & Chen, 2009; Webb and Soh, 2007).

Another major stream of related works is about defensive techniques against cheating. In light of studies on protective measures, diverse methods have been suggested, including a guideline (Jeng & Lee, 2013), algorithm design (Mönch et al., 2006), and a framework for modeling (Ferretti, 2008).

In social sciences, the most actively studied topic regarding cheating in online games is about explaining which motivation is to make users cheat. Yee (2006) suggests ten motivation components that are grouped into three overarching components: achievement (advancement, mechanics and competition), social (socializing, relationship and teamwork), and immersion (discovery, role-playing, customization and escapism). Schwierien and Weichselbaumer (2010) reveal that competing for a desired reward affects not only an individual's performance, but also their tendency to cheat. Major results of their experiments show that poor performers notably increase their cheating behavior during competition, being an effort to retain a chance of winning or a face-saving strategy. Chen and Wu (2015) conclude that the frequency of gaming with strangers has a remarkably high correlation with the frequency of cheating in online games. The effect of anonymity on cheating was discovered to be mediated by the characteristics of groups; female gamers have a higher level of mediation than male gamers, whereas male gamers generally cheat more often than female gamers.

In addition, in social sciences, research regarding the social activities among users and the cultural aspects of online games also take an important place. Taylor (2009) argues that massive multiplayer online games (MMOGs) can be considered social spaces, in which thousands of players take part in a virtual world simultaneously. The author finds multiplayer gaming life living on the borders, hence in the

intersection of online and offline space, as players get engaged in complex social networks that take place both in online and offline spaces. Zhong (2011) explores how social activities and playtime in online games affect their online and offline social capital. It is argued that social activities can increase online and offline social capital to a certain degree. In contrast, the playtime of a game can negatively influence online and offline social capital.

The method of cheating detection is a crucially important research topic for the online game literature. Many existing studies focus on defining behavioral “patterns” that are valuable in finding cheaters and constructing a detection mechanism with such patterns. Our study is proximate to multi-boxing and bot detection in that users use automated programs (bots) with multiple types of access (multi-boxing). While there currently exist a great deal of literature regarding bot detection, only few studies address multi-boxing detection. Table 1 summarizes the previous studies related to bot detection. Some studies suggest using CAPTCHA tests during a game to identify whether an avatar is actually controlled by a person or not (Golle and Ducheneaut, 2005; Von Ahn et al., 2003; Yampolskiy and Govindaraju, 2008). Although, CAPTCHA test is effective, it disturbs the game play and diminishes players’ feelings of immersion in the game (Chen et al., 2008). There are studies using traffic information to detect bots (Chen et al., 2009; Hilaire et al., 2010). In such traffic analyses, specific features of traffic such as regularity, burstiness, and sensitivity are used. User behavior analysis utilizes different patterns between programmed bot behaviors and human behaviors. In such regard, various detection guidelines are proposed highly depending on the rules and environment of the game (Thawonmas et al., 2008; Chen and Hong, 2007; Yeung

et al., 2006; Varvello and Voelker, 2010; Yan, 2009; Ahmad et al., 2009). Some studies focus on different moving patterns between humans and bots (Van Kesteren et al., 2009; Mitterhofer et al., 2009; Thawonmas et al., 2007). Interaction patterns using hardware interface, i.e., inputs using the mouse and keyboard, are also used in bot detection studies (Kim et al., 2005; Gianvecchio et al., 2009).

Table 1. Recent Research on Bot Detection

Category	Adapted Method	Definition/key Paper	Key Idea	Merits/demerits
Client side detection	CAPTCHA analysis	Detection method with challenge–response test (Yampolskiy and Govindaraju, 2008; Golle and Ducheneaut, 2005)	- Challenge–response method	- Merit: high speed - Demerit: reducing immersion of players in online game, low feasibility
Network side detection	Traffic Analysis	Detection method based on network traffic analysis (Chen et al., 2009; Hilaire et al., 2010)	- Command packets timing analysis - Traffic explosiveness analysis - Networks response analysis - Data length analysis - Traffic interval time analysis	- Merit: high utilization of the other algorithms like decision tree - Demerit: low accuracy rate

Server side detection	User behavior analysis	Detection method based on user behavior pattern in game play (Thawonmas et al., 2008; Chen and Hong, 2007; Yeung et al., 2006; Varvello and Voelker, 2010; Yan, 2009; Ahmad, 2009)	- Idle time analysis - Social connection analysis (chatting, trade)f	- Merit: high accuracy rate, high detection rate, high availability
	Moving path analysis	Detection method based on patterns and zones of moving path analysis (Kesteren et al., 2009; Mitterhofer et al., 2009; Thawonmas et al., 2007)	- Coordinate analysis - Zone analysis	- Merit: high feasibility - Demerit: low accuracy rate
	Human observation proofs analysis	Detection method with keyboard and mouse input patterns analysis (Kim et al., 2005; Gianvecchio et al., 2009)	- User inputs observation - Windows event sequence analysis	- Merit: high accuracy rate - Demerit: low feasibility

Note. Adapted from Kang et al. (2013).

The debate over whether cheating in video games is positive or negative continues in the industry as well as in the academia (Consalvo, 2009). The common reasons for the claims that cheating has negative effects on the video game is: 1) cheating undermines the notion of fairness in the game by giving undesirable advantages to cheaters, 2) cheaters destroy the game economies by depleting in-game contents and creating a large imbalance among users (Thawonmas et al., 2008; Gianvecchio et al., 2009; Yan and Randell, 2009; Kang et al., 2013). On the other hand, the studies which argue that cheating in the video game has rather positive effects are based on the fact that cheating complements the underlying imperfections and limitations of initial game design. According to Consalvo (2006; 2009), not all games can be consummate. Therefore, sometimes, players get stuck, feel bored, or have to repeat meaningless actions during their playtime. In such situation, cheating can improve the user's game experience by supplementing the game's "bad design" and prevent users from leaving (Rossignol, 2009; Aboukhadijeh, 2009; Consalvo 2009). Also, there are claims that cheating can provide other enjoyable aspects to the game by promoting user creativity in plays (Green and Kaufman, 2015; Gino and Wiltermuth, 2014; Ejsing-Duun et al., 2013). In addition, there are studies which argue that cheating has a positive effect in game-like contexts other than video games. Gal-Oz and Zuckerman (2015) argue that cheating behavior in the "gamified" fitness application could actually be beneficial as they it can encourage physical activity. Kirman et al. (2012) suggest that mischievous activities could serve a vital and positive social role, in games and other contexts. In conclusion, the negative effects of cheating appear in terms of relationships to other

users, and the positive effects of cheating appear in aspects of improving the individual player's overall game experience.

Besides, impacts of cheating or unethical behavior are an important research question in a number of fields; there exist a number of prior studies in the context of e-commerce, information good markets and IT service. One of the other works which is closely related to online game cheating is piracy in the digital good market. With respect to piracy on the digital good market, a large number of researchers argue that piracy has a negative effect on legitimate sales of digital contents. Ma et al. (2011) find out that pre-release movie piracy leads to a 19.1% decrease in box office revenue in comparison to the piracy that occurs post-release. Hennig-Thurau et al. (2007) discover that movie piracy in Germany gives rise to substantial cannibalization of theater visits, DVD purchases and rentals, being responsible for yearly revenue losses of \$300 million. Rob and Waldfogel (2007) present that the first piracy on movie consumption decreases legitimate consumption by about 1 unit. On the other hand, there are studies that show that piracy has no effect on legitimate sales. Smith and Telang (2009) examine that there is possibility of piracy on television broadcast contents having no influence towards post-broadcast DVD sales. Bounie et al. (2006) explain that piracy has no statistically significant effect on box office revenue.

From the review of previous studies, I have found several significant implications for the research. First, the study about cheating or unethical behaviors in online games is in its infantile stage compared to other areas in which much research has already been performed, such as e-commerce, information good markets and IT service. Second, there exist scant research works to analyze whether, and how

much, online game cheating affects firms' sales and users' behaviors from the perspective of empirical methods with real field data. Third, existing cheating detection methods require large amounts of transaction data processing or additional development, and as a result, they make it difficult for many companies to utilize such methods in real-world settings.

3. Data

I collected data for three variables from Korean online game provider: user ID, monthly playtime of each user, and monthly cash item purchase of each user from February 2014 to January 2016. I limited the number of variables used in the analysis to address the data availability issue. Generally, allowing for the exceptions for giant game companies, most game providers initially design their databases with primary focus on operation rather than analysis. Therefore, it is common that game companies are not able to provide sufficient data for analysis. Even if companies can extract data, acquiring it requires a huge amount of computing resources and puts a tremendous burden on the database. I tried to address this data availability issue and suggest a method that companies with scarce data can easily apply to their systems without loss of generality. It should be noted that user ID, playtime and purchase are essential variables that most providers consider when designing databases because the three variables are absolutely indispensable for basic indicator analysis.

I conducted most of analyses on a monthly basis, because the results of analyses based on daily, weekly, and monthly data were similar. When analyzing monthly unit, computing power can be saved, compared to conducting daily or weekly unit

based analysis. If the time span of the data is short, the data of weekly or daily unit could be more proper. However, if the time span of data is rather long as in our case, employing monthly unit is more efficient in terms of computing power.

Total number of registered users is 80,368 and 30% of them (Approximately 24,000) are active users who play the game on regular basis. A small number of top 10% users (8,000) hold 80% of the playtime and top 2.9% users take up to 80% of the revenue. This implies that a few number of users could have large impact and show their incomparable loyalty to the game. Such trend can be easily observed in other games as well (Swrve, 2016). Moreover, it could mean that cross-subsidization effects in gaming platforms are comparatively larger than those of other platform business.

4. Hypotheses

In this section, I outline the empirical questions addressed in this study and discuss the theoretical rationale for each question.

First, I hypothesize that cheating in online games will increase the user's playtime and purchase. According to self-perception theory, when there is no previous attitude due to a lack of experience, people develop their attitudes by observing their own behavior and concluding what attitudes must have caused it (Bem, 1972). One typical example is the foot-in-the-door technique, which is a widely used marketing technique for persuading target customers to buy products. The basic premise of this technique is that, once a person complies with a relatively trivial request, he or she will be more likely to comply with a more substantial request,

which is rather related to the original request. The idea is that the initial commitment on the small request will have influence on one's self-image, therefore giving reasons for agreeing with the subsequent, larger request. Meanwhile, according to Yee (2006), there are ten motivational sub-components that can be grouped into three overarching components for people playing online games: achievement (advancement, mechanics and competition), social (socializing, relationship and teamwork), and immersion (discovery, role-playing, customization and escapism). Among these motivational sub-components, cheating, playtime and purchase are related to achievement, particularly advancing and competition (Kabus et al., 2005; Chen et al., 2005; Yee, 2006; Xiao et al, 2009). In other words, users spend more time, buy items or engage in cheating because of their desire to gain power, progress rapidly, accumulate in-game symbols of status, and successfully compete with others. MMORPG is a virtual community that many users enjoy together and achievement is one of the factors that makes the relative superiority among users feel immersed in the game (Chen et al., 2006, Chen et al., 2007). As a result, when users cheat, the attitude of achievement is reinforced, and more actions such as play or purchase are taken to satisfy this attitude. More specifically, people observe their own behaviors (paying attention to and complying with the cheating) and the context in which they behave (incentive to achieve more than others), and thus infer they must have a preference for those incentives and behave accordingly. For such reasons, I expect cheating will increase users' involvement in terms of playtime and purchase.

H1: Cheating in online games will increase the user's playtime.

H2: Cheating in online games will increase the user's purchase.

Second, I hypothesize that cheating users will have a negative impact on other users. Cheating can be defined as the act of destroying the rules of the game that everyone has to obey, which are commonly predetermined by the developer. Cheating in online games has a negative impact on users who invested time, money and emotional attachment to raise their avatars (Aboukhadijeh, 2009). In other words, cheating behaviors can negatively influence users that do not cheat by making them feel unjust or unfair. According to Adams (1963), people compare their inputs and outputs to those of others in organizations when determining “equity.” As cheaters outperform non-cheaters with relatively tiny amount of inputs, non-cheaters are prone to feel deprived and undeserved. Such “relative deprivation” that leads to perceived injustice; it should be noted that “deprivation is perceived relationally.” To put it more measurably, two people, hypothetically A and B, tend to assume that “distributive justice” is achieved when:

$$\frac{A's\ rewards - A's\ costs}{A's\ investments} = \frac{B's\ rewards - B's\ costs}{B's\ investment}$$

Hence, under the existence of cheaters, most non-cheaters are likely to perceive “relative deprivation,” leading to distributive injustice among users in gaming community (Adams 1965). The “relative deprivation” will make the people leave the group (Carrell and Dittrich, 1978). In this respect, I anticipate cheating will have a negative impact on other users' playtime and purchase.

H3. Cheating in online games will decrease normal user's playtime.

H4. Cheating in online games will decrease normal user's purchase.

Third, I hypothesize that cheating users will have a longer life-span than regular users. I expect cheating to increase users' playtime and purchase. On that extension, I expect cheating will increase the user's sunk cost. This is because cheating users are expected to spend more time and money. High sunk cost increases the lock-in effect (Shapiro and Varian, 2013). On the psychological side, someone can argue that cheating users can lose interest in games more quickly because they feel guilty. However, according to neutralization theory, cheating users are likely to mitigate guilt by believing that they make a big contribution to the game, because they make more purchases. Neutralization theory is a psychological theory that people tend to avoid "inner protests" when they take action, or are at the point to do something that they perceive as wrong (Siponen and Vance, 2010). Based on these reasons, I expect cheating will also increase users' life span.

H5. Cheating users will have a longer life span than regular users.

5. Method

5.1. Cheating Identification

Existing methodologies related to our research include rule-based method and data mining-based method. The rule-based method recognizes specific patterns, which are used in cheating by using domain knowledge, and sets its own identification rule in order to identify cheaters. With rule-based method, flexible criteria can be designed to find any usage patterns in a detailed user behavior history. Also, rule-based method works best with data having explicit information, in which fraud-detecting criteria can be referred as rules. (Kou et al., 2004).

There are two reasons why I used rule-based method over data mining-based method. First, since the data mining-based method requires enough data quality and quantity (Phua et al., 2010; Cox, 1997), it cannot be used in cases in which there are not sufficient data. One of our goals is to develop methods for game companies who are unable to gather large-scale datasets. For this reason, I decided to use a rule-based approach, which can be performed utilizing minimum number of data. Second, I chose the rule-based approach to avoid the unlabeled data problem. With respect to cheating prediction model, one of the state-of-the-art can be a supervised learning approach with deep learning techniques. Deep learning has come out to be very good at addressing intricate structures in high-dimensional data and has dramatically improved the state-of-the-art results in a number of domains (LeCun et al., 2015). I also have prior experience using deep learning to build models that forecast game users' churn and purchase, and the results were remarkable. However, supervised learning usually cannot be used for cheating identification because of unlabeled data problem. In order to use the supervised learning method, it is necessary to have a large number of labeled training data instances, those conveying prior identification information of cheaters. (Phua et al., 2010; Kou et al., 2004). The user's purchase or churn can be easily identified by pulling out past records, but it is not the case in identifying cheaters.

Before establishing a rule to identify cheating users, it is necessary to clarify what types of cheating behaviors take place in the game. In this paper, I focus on two major types of cheating that happen simultaneously: multiboxing and game bots. Multiboxing refers to the activity of playing as multiple separate avatars at the same time in MMORPGs. It has appeared due to the increasing hardware

performance of computers and the emergence of emulators that can run online games or mobile games in multiple instances at the same time. Multiboxing is a relatively recent concept compared to other cheating behaviors, but it is growing rapidly in recent years. On the other hand, game bots, which have appeared earlier than multiboxing, have been actively studied in the academia. The bot is a kind of an agent software that plays video games in replacement of the humans (Video game bot, n.d.). Using bots in MMORPGs allows users to grow their avatars faster than others because they can automatically make their avatars to hunt or battle, even when they are not actually playing the game.

Figure 1 is an example of how cheaters use multiboxing and bots in the game. Cheaters usually run multiple instances simultaneously within their computational resource bounds. Then, they use game bots to automatically control avatars in multiple instances. If cheating users do not utilize game bots, it is usually highly inefficient since only one avatar can be controlled by a user at a time. Furthermore, another reason why the cheating users use multiboxing and bots together lies on the functional limitations of bots. In MMORPG, the users need to win much stronger antagonists in order to gain better rewards. However, if bots are used, it is much harder to beat stronger antagonists because the bots cannot effectively respond to diverse situations as humans do. Therefore, in order to fight with stronger antagonists, the game players use a way of cooperating with many different avatars by using multiboxing. To sum up, cheaters of the game log in with a number of different IDs and use various avatars at the same time by using multiboxing and bots. Furthermore, it should be noted that such trend can be frequently observed in other games as well.

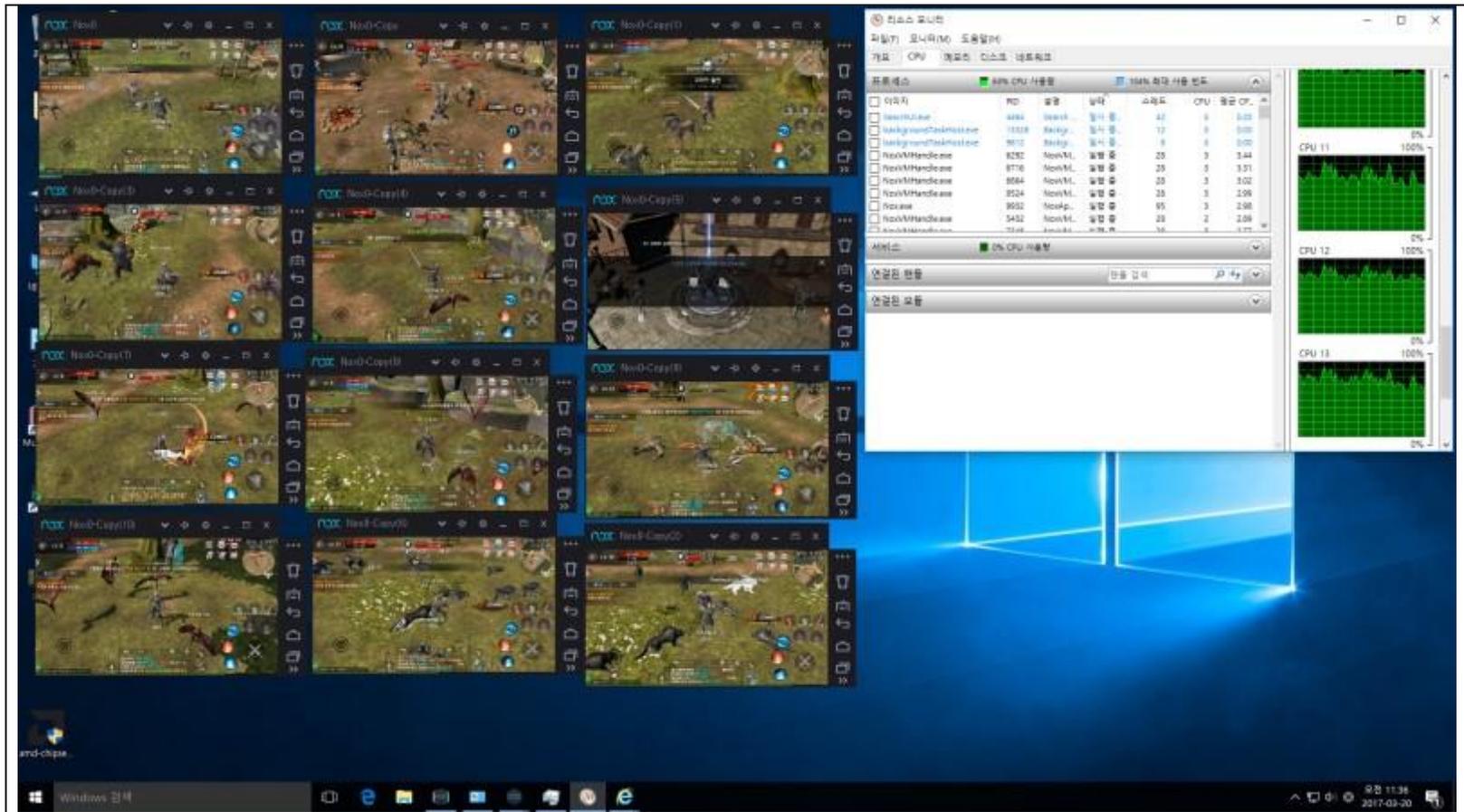


Figure 1. An Example of Multi-boxing and Bots

In this study, I made “rules” in order to identify who cheaters are by using distinctive characteristics of cheaters who use cheating tools (multiboxing and bots). To be more specific, if the cheaters have multiple IDs and play with them, these IDs show extremely similar playtime patterns to each other.

Figure 2, 3 and 4 below show different playtime patterns of the game users. In the figures, the x-axis refers to time (i.e., month) and the y-axis refers to the sum of playtime during each month.

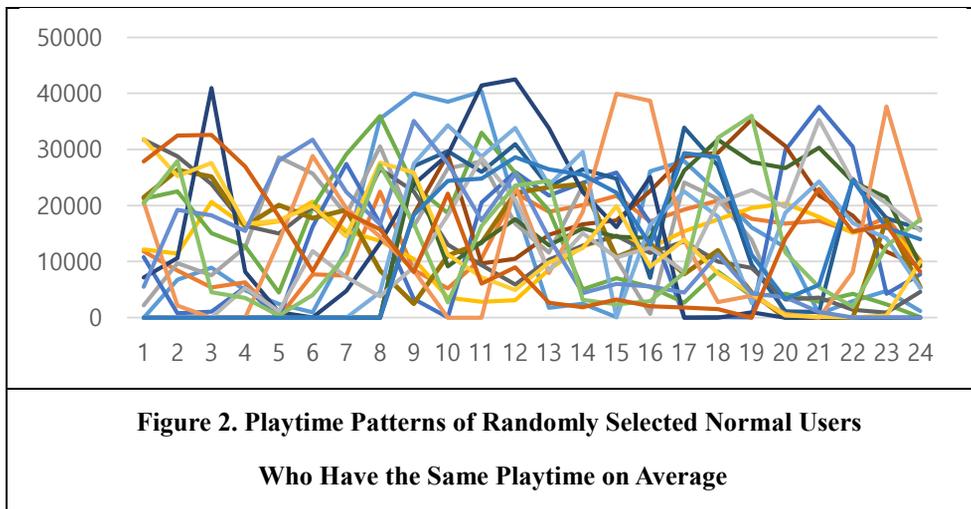


Figure 2 displays playing patterns of twenty randomly sampled normal-cheating users, who have the same playtime on average. I can find that each of the normal users has extremely diverse playtime patterns and those playtime patterns seem to barely overlap one another.

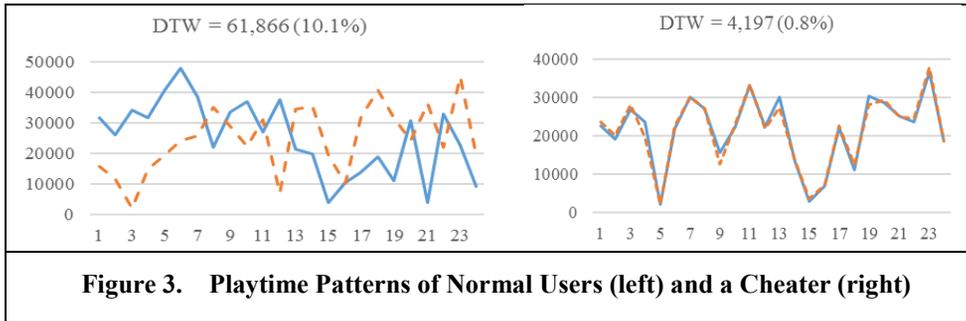


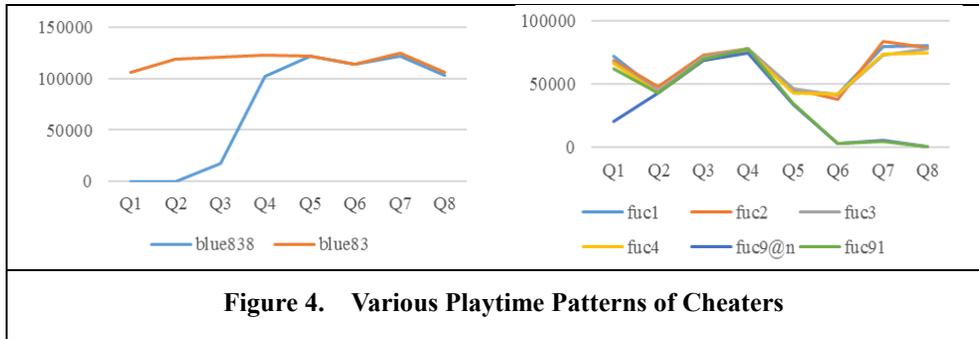
Figure 3. Playtime Patterns of Normal Users (left) and a Cheater (right)

The left graph in Figure 3 shows playtime patterns of two different users who have the same average playtime. Generally, users who do not use hacking tools show such different playtime patterns. In contrast, the right graph in Figure 3 represents playtime patterns of a single cheater who uses two different IDs at the same time. It seems that playing patterns of a cheater are nearly identical to each other, almost indiscernible.

I used Dynamic Time Warping (DTW) method in order to capture the playtime patterns of cheaters. DTW is widely used in anomaly detection tasks, although it is also used in various fields. It is mainly used to calculate the similarity of time series data or signal (or wave) data, and group the behavioral patterns or different users into similar clusters based on the rule made using various domain knowledge (Lee 2017; Vy and Anh, 2016; Izakian et al., 2015; Boulnemour et al., 2016; Carvalho et al., 2013; Salvador, 2004; Benkabou et al., 2017). I also use DTW to cluster the IDs of a cheating user playing multiple avatars at the same time.

DTW is a robust distance measure for time series, permitting similar shapes to match although they are out of phase in the time axis. (Keogh and Ratanamahatana, 2005). It can be used to calculate the distance between two different time-series

datasets (Berndt and Clifford, 1994). In other words, the degree of differences between two time-series graphs can be represented numerically by using DTW. For example, in Figure 3, the DTW score of two different users who have similar playtime on average is 61,899 (left in the figure), which is relatively high. However, the DTW scores of two different IDs, which are owned by one cheater, are only 4,197 (right in the figure). In order to easily compare DTW scores, I used standardized DTW scores (by dividing DTW score by average of playtime between IDs) as seen in the parenthesis beside DTW scores in Figure 3. I also calculated and compared DTW scores among different IDs every month to identify diverse types of cheaters, such as those who use hacking tools for a certain period of time only and who add new IDs in the middle of game playing with existing IDs (see Figure 4).



I set another rule which can complement the DTW score. As seen in Figure 4, cheaters tend to use slightly different IDs for the sake of memorability. For example, they make many IDs by changing additional numbers based on same characters such as ‘blue838’ and ‘blue83’. I used those characteristics when DTW scores could not assure whether some particular IDs are owned by one cheater or not. The method of using string distance among IDs or texts to guess an

individual's identity is used in various fields such as data linkage (as known as entity resolution), which refers to the task of searching records that are essentially the same entity across different data sources (Brizan and Tansel, 2006; Malhotra et al., 2012; Goga, 2014). In this study, I used an algorithm named JWD (Jaro-Winkler distance) to compute similarities between IDs. Jaro-Winkler distance is a measure of similarity between two strings and is designed and well-fitted for short strings such as people's names (Winkler, 1990). Because IDs are composed of short strings, JWD can be deemed an appropriate way to calculate distances between IDs.

Figure 5 shows the result from JWD analysis between IDs. In this figure, the user named 'bluelet' has 4 more IDs, 'bluelett', 'bluele', 'bluelette' and 'blueletter'. From our experience, if there are IDs which have JWD score below 0.1, they are highly likely to be cheating IDs which are owned by one user. For example, 'bluelet' and 'blue83' do not belong to the same user because their distance score over 0.1, 0.253968.

	bluelet	devil8	leekw015	demon6	blue83	lok8162	8697ksk@	ru
bluelet	0	0.460317	0.39881	0.563492	0.253968	0.571429	1	0
bluelett	0.041667	0.638889	0.416667	0.569444	0.277778	0.577381	1	0.
bluele	0.047619	0.444444	0.375	0.555556	0.222222	0.563492	1	0.
bluelette	0.074074	0.648148	0.430556	0.574074	0.296296	0.582011	1	0.
blueletter	0.1	0.655556	0.441667	0.577778	0.311111	0.585714	1	0.
blue83	0.253968	0.444444	0.472222	0.555556	0	0.460317	1	0.
bluecill00	0.261905	0.566667	0.441667	0.577778	0.311111	0.585714	1	0.
leetw921	0.309524	0.569444	0.25	0.569444	0.472222	0.509921	0.587963	0.
leetw640	0.309524	0.569444	0.25	0.472222	0.472222	0.488095	1	0.
xcruelx	0.380952	0.563492	0.577381	1	0.460317	1	1	0.
dwlee90	0.380952	0.468254	0.320238	0.460317	0.460317	0.571429	0.582011	0.
ghlee10	0.380952	0.626984	0.286905	0.563492	0.460317	0.47619	1	0.

Figure 5. Examples of Jaro-Winkler Distance

Even though JWD scores between IDs are not a perfect criterion to identify cheaters but are quite useful in the aspect of practical usage. From results of analysis that I performed, I could identify more than 70% of cheaters by calculating similarities between IDs. However, although JWD analysis is a good method for cheating identifications especially for multi-ID usage, there is a critical reason why this method cannot be used alone. JWD analysis tends to misidentify normal users as cheaters if it is used solely. For this reason, this method is best suited for complementing ways to identify cheaters. In this context, I used JWD analysis when I roughly choose and guess cheater groups before precise analysis is carried out. I also conducted JWD analysis when I am not sure whether some particular IDs are owned by a single cheater or not with DTW analysis only.

5.2. Measurement of the Cheating Usage Effect

One of the methods widely used to measure causal effects of time-series data is quasi-experiment using DID (Difference in Differences) (Lechner, 2011; Dehejia et al., 2002). A quasi-experiment is an empirical study employed to measure the causal impact of an intervention on its target groups without random assignment (Quasi-experiment, n.d.).

Since the work by Ashenfelter and Card (1985), Difference in Differences (DID) are commonly used to calculate the effect of sudden events on time-series data (Imbens and Wooldridge, 2007). Difference in differences measures the treatment effect on an outcome by comparing the average fluctuation over time in the dependent variable among the treatment group with that among the controlled

group (Difference in differences, n.d.). In the simplest setup, outcomes are recorded for two groups in two separate time periods. The treatment group is exposed to a certain treatment in the second period, but not in the first period. The controlled group is not under the influence of the treatment during both first and second period. For the case in which the same units within a group are observed in each time period, the average gain in the latter group is subtracted from that in the former group. This eliminates the bias in second period's comparisons between the groups that could be arising from inherent differences between two groups, as well as biases from comparisons over time in the treatment group that could be the consecutive result of trends (Imbens and Wooldridge, 2007).

Although one of the objectives of using DID is to alleviate the effects of external factors and selection bias, which is highly dependent upon how the treatment group is chosen, it is still prone to bear certain biases (e.g. mean regression, reverse causality, and omitted variable bias). For this reason, in quasi-experiment, an additional control technique that mitigates self-selection between the experimental group and the control group are usually performed before DID analysis. One of the most popular methods for such controlling is Propensity Score Matching (PSM). However, since there are not sufficient explanatory variables which can be employed to match experimental and control groups using PSM, we used DTW in order to select control groups that have similar time series patterns of playtime and purchase with experimental group. The method that find the best matched control groups with time series data using DTW has recently started to be used in domains such as marketing, finance, and medicine (Schmitt et al., 2017; Li et al., 2015; Larsen, 2016; Yuan, 2014).

The reason I can use DTW instead of other control methods such as Propensity Score Matching (PSM) in quasi-experiment is because our experiment has some characteristics of natural experiments. According to information gained from the game provider, very few distributors personally communicate with normal players using in-game chat and thus it is hard to know where and when they will distribute hacking tools. Even cheating users tend to be reluctant to social activities and behave secretly as they fear other users' reports on their cheating behaviors. If they are known to be cheaters, the game provider can kick out the cheaters and remove their avatars that took hundreds to thousands of hours to grow. Also, cheaters risk social relations when cheating since there exist social penalties involved with it (Blackburn et al., 2014). Therefore, the only way to meet hacking tool distributors is encountering them by chance in the game field during gameplay. A lot of users want to get a hacking tool. This is because using a hacking tool greatly ameliorates game playing efficiency and reduces time consumption. However, in reality, obtaining a hacking tool is highly dependent upon one single factor, luck. I tried our best to get a hacking tool for the study, but failed like other users did. Consequently, hacking tools can only be obtained with luck and users cannot control the conditions for owning a hacking tool. Hence, I think that this situation is similar to the setting in the natural experiment, in which most conditions cannot be controlled artificially. For this reason, I only controlled some characteristics, such as playtime and the purchase of experimental and control groups through DTW.

In addition, I tested whether it is reasonable to use playtime and purchase data when matching control groups using DTW in our experiment. I want to make sure

that users with similar playtime and purchase patterns show similar playtime and purchase patterns in the future if there are no external factors. To this end, I performed Autoregressive (AR) model to verify the validity of selecting a control group with the user's playtime and purchase. For more details, using Partial Autocorrelation Function (PACF), I confirmed that lagged purchases and playtime variables belonging to the pre-period are significant input variables in predicting each of playtime and purchase after the pre-period (Greene, 2007). The regression results also confirm that I can predict the user's future playtime and purchase fairly well with only current playtime and purchase; in the regression analysis, lagged playtime and purchase variables in pre-period are used as independent variables and each playtime and purchase in the first period of post-period are used as dependent variables. It should be noted that in previous studies, playtime and purchase are dominant features in game research oftentimes. Especially, in the model which predicts the user's playtime and purchase, the playtime and purchase records of the user are the most important variables (Hadiji et al., 2014; Drachen et al., 2016; Mahlmann et al., 2010; Sifa et al., 2015). The fact that playtime and purchase in games have such autoregressive tendencies is also a part of the consensus among game providers. To sum up, the results of robustness check confirm that if normal users have a similar pattern of playtime and purchase in advance, they would show similar playtime and purchase patterns in the post-period to some extent, provided they do not use hacking tools. In this context, the way I used to group users' playtime and purchase patterns with DTW seems to be useful in solving the problem of self-selection bias.

In this study, I tested whether each of the user groups changed their playtime and purchase patterns in post-period depending on the usage of hacking tools. I also measured the changing amount of playtime and purchase affected by hacking tool usage by conducting a quasi-experiment. For more details on the quasi-experiment that I performed, as experimental group, I selected all of the 25 users who do not use hacking tools at first (pre-period) then start using them later (post-period). As a control group, I also selected 25 users who have similar playtime and purchase patterns in pre-period compared with experimental group by using DTW. In this process, daily playtime and weekly purchases are used. The reason for using weekly data rather than daily for purchase is that the daily purchase dataset is sparse. In other words, in the case of daily purchase, most of the data is 0, which may cause dangerous biases in the analysis results (Greenland et al., 2016). The pre-period and post-period, respectively, are set at three months, which is a result of considering the business operation aspect of the provider establishing major marketing strategies on a quarterly basis. The figure 6 shows a brief overview of the quasi-experiment I have performed.

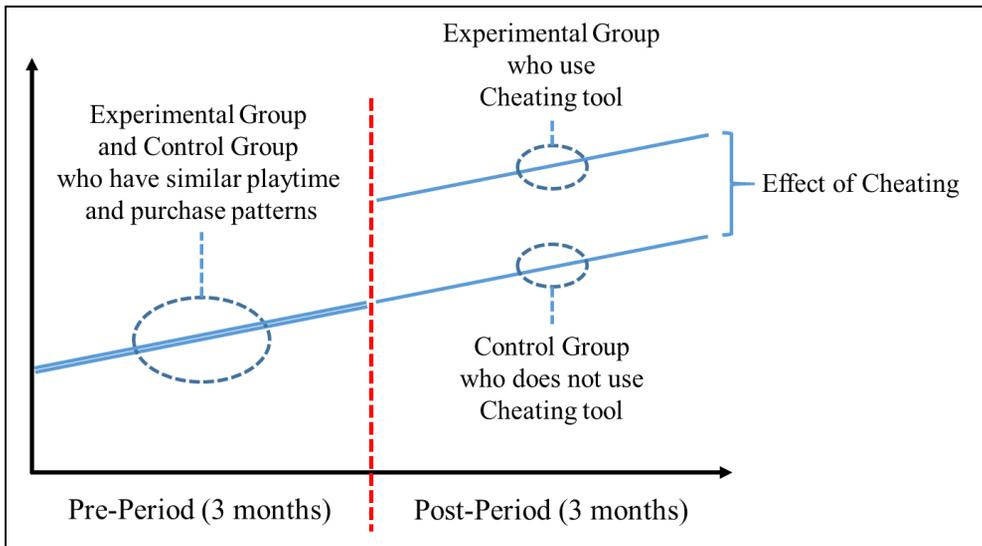


Figure 6. Overview of the Quasi-experiment

6. Result

6.1. Cheating Identification

I found that 207 game users in possession of 1,026 IDs are cheaters. It was also shown that they tend to log in with five different IDs at the same time, on average. One interesting point is that although they are only 0.25% of the whole registered users of the game, but they are mostly VIP users who holds 6% of playtime and 12% of the total revenues.

6.2. Measurement of the Cheating Usage Effect

In Figure 7 and Table 2, it is shown how game users' playtime pattern and purchase pattern changed before and after they started using hacking tools for three months respectively (a total of six months). As a result of DID analysis, it was revealed that

users who used hacking tools had dramatically increased their playtime (18,504 minutes, 102%) and purchase (23,642 won = \$ 20, 79%), compared to those who did not use hacking tools.

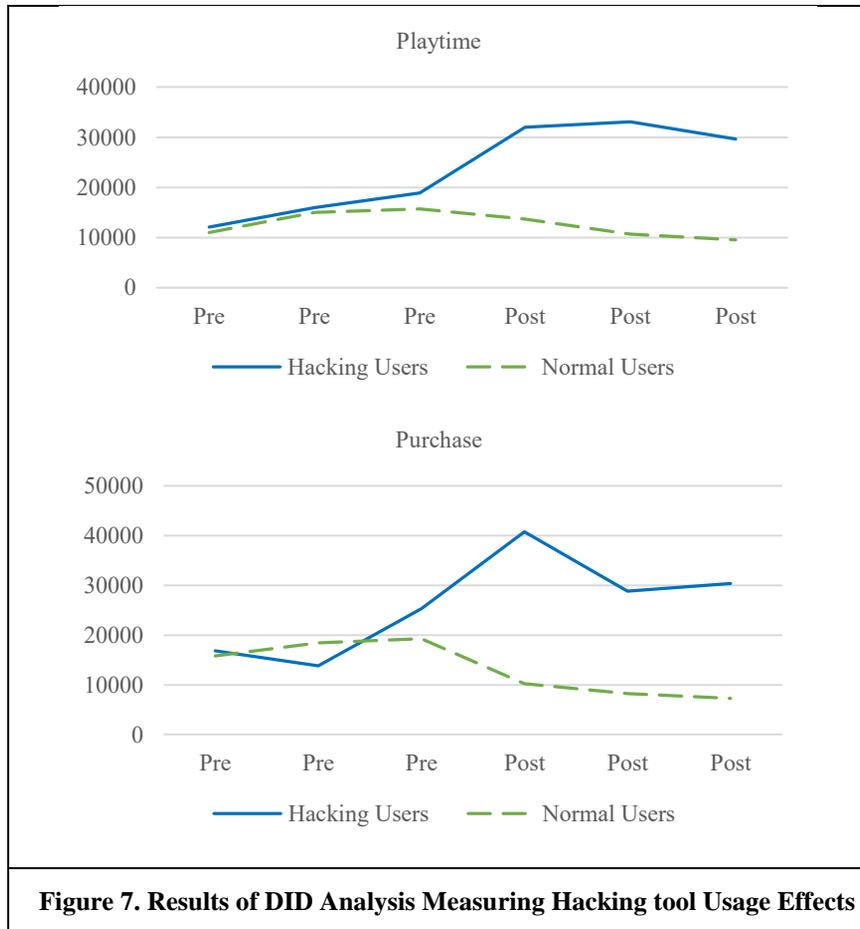


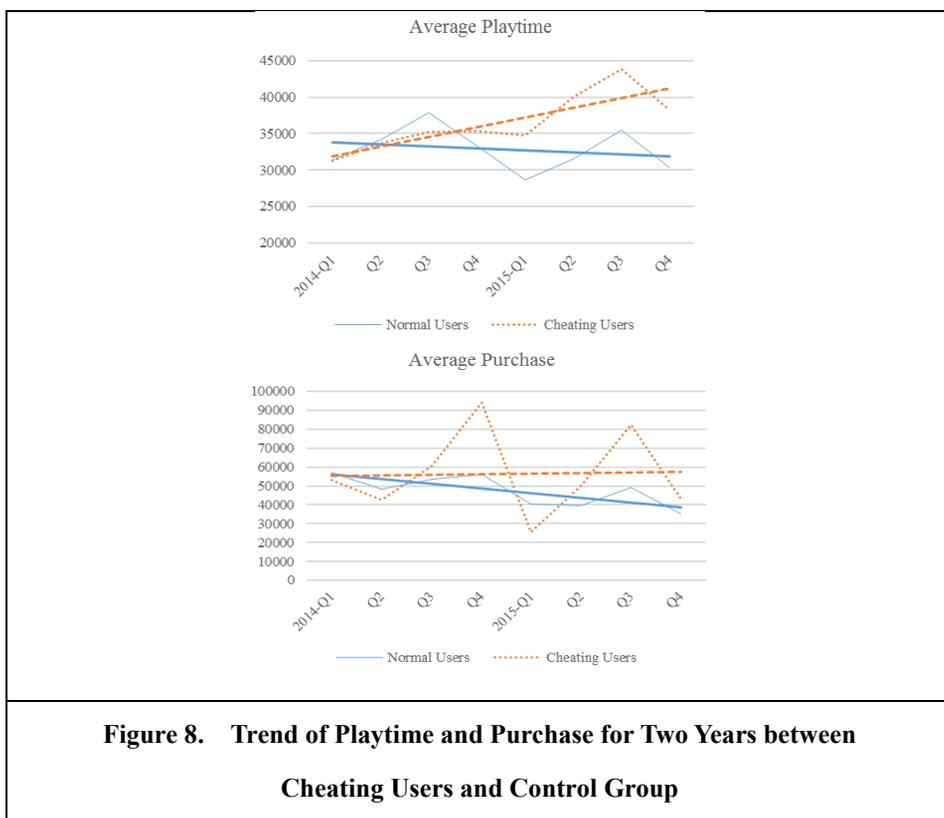
Figure 7. Results of DID Analysis Measuring Hacking tool Usage Effects

Table 2. Results of DID Analysis Measuring Cheating tool Usage Effects		
Coefficients	Playtime	Purchase
(Intercept)	13,930 (***)	17,543 (***)
Treated	1,736	1,090
Time	-2,006 (***)	-8,946 (***)
Difference in Differences	18,504 (***)	23,642 (***)

7. Additional Analysis

7.1. Life Span of Cheating Users

Generally, the expected lifespan of cheaters can be shortened since they quickly use up the game contents by using hacking tools. For this reason, I checked whether the effects of hacking tools are just short-lived or not. I compared play patterns of the cheating group and the control group with similar average playtime and purchase early in the observation period with each other. Surprisingly, according to our results, cheaters tend to keep spending playtime and purchase steadily compared to non-cheaters for about two years (see Figure 8). It explains that the effects of hacking tools are not short-lived; they persist for a quite a long time.



7.2. Granger Causality Test

Additionally, I tested whether the presence of cheating users would have a negative impact on other normal users. Figure 9 compares the playtime of cheating users with the playtime and purchases of normal users respectively. By observing the time series shown in Figure 9, I cannot judge whether these two trends affect each other or not. Therefore, I performed a granger causality test to determine whether cheating users' time series is useful in forecasting other normal users' time series. To be more specific, I tested whether the playtime of cheating users granger cause playtime and purchases of normal users. In the granger causality test, I used monthly playtime and purchase records of both non-cheating and cheating users.

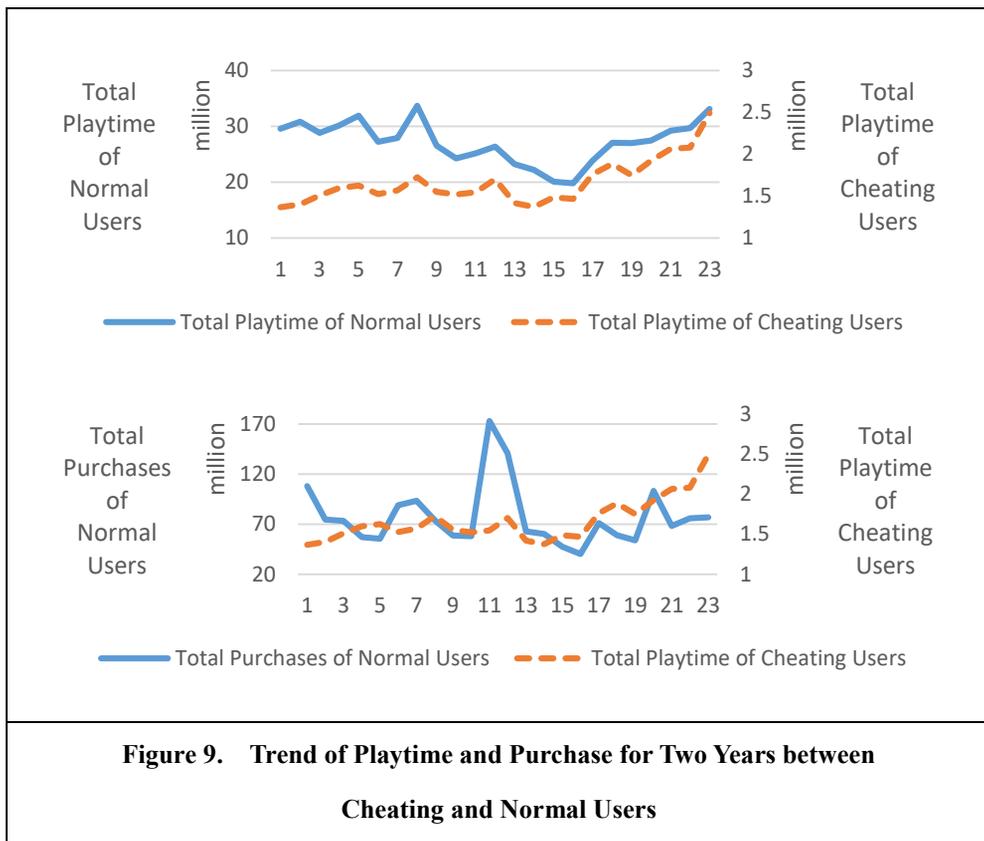


Table 3 shows the results of the granger causality test. The lagging term refers to how many terms back down the granger causality test I want to test for serial correlation. As a result, playtime and purchases of cheating users cannot provide statistically significant information about future values of non-cheating users' playtime and purchases. In other words, cheating users' activity does not affect non-cheating users' playtime or purchases.

Table 3. Results of Granger Causality Test		
	Cheating Users' Playtime Granger Cause Normal Users' Playtime	Cheating Users' Playtime Granger Cause Normal Users' Purchase
Number of Order (lagging term)	Pr(>F)	Pr(>F)
1	0.1401	0.3458
2	0.3663	0.1034
3	0.4378	0.07134
4	0.6097	0.205
5	0.6908	0.3734
6	0.489	0.5013

8. Discussion and Conclusion

In this study, I aim to identify cheaters with a modest amount of data and examine how hacking tools affect users' playtime and purchase behavior. As a result, I have found that there are 207 users (0.25% of registered users) who use hacking tools and they are highly valued users who hold approximately 12% of the whole revenue. Moreover, it was found that a user's playtime and purchase increased by

102% and 79% respectively, right after the user start to use hacking tools. I also showed that the effects of using hacking tools are not just short-lived.

In order to evaluate the accuracy of the results, I used the heuristic method of observing the users by which the person in charge of the game operation in the provider. Because of the unlabeled data problem, I could not perform typical evaluation methods such as cross-validation using training and test dataset. Furthermore, since the software used for multiboxing assigns a dynamic IP to each instance, verification using IP addresses could not be used. As a result, I confirmed that users classified as cheating users are actual cheating users, except for some users who play close to 24 hours a day on average with a certain ID. In the case of IDs that were classified as exceptions, I was not able to find a unique pattern to distinguish them as the same user or different users, as they were connected 24 hours a day, during their playing time.

I conjecture that cheating increases a user's playtime and purchase since cheating enhances user's game experience. According to Consalvo (2006), there are four reasons why users cheat in a game: they are stuck, they eager to “play God,” they are bored with playing the game, or they desire to be a jerk. I see our case to mostly belong to the third reason: users got bored with the game due to systematic reasons inherent in the game. The game I analyzed has been around for 10 years. The provider tries to add new contents through additional updates, but the structure of the game is outdated. Compared to recent games that emphasize speed and variety of enjoyment, the design of the game focuses on raising dozens of avatars through time-consuming and repetitive activities. Therefore, for some users who have been playing games for a long time, the game seems rather tedious and dull. I observed

the pattern of 207 users identified as cheaters, and analyzed the reaction of the user community to confirm such assumption. In this situation, utilizing cheating tools could reduce the time-consuming activities of the users and increase the speed of the game, thereby enhancing the users' game experience. As a result, users seem to be more actively engaged in the game through cheating, and spend more time and money. Similar results relating cheating behavior and game experience can be observed in previous studies as well (Consalvo, 2009; Rossignol, 2009; Aboukhadijeh, 2011).

The reason for the cheating effect lasting for long term seems to be that the game design did not improve through the update, constantly showing some limitations. In general, bots or multiboxing accelerates content consumption and reduces a lifespan of the game (Thawonmas et al., 2008; Gianvecchio et al., 2009; Yan and Randell, 2009; Kang et al., 2013). Recently, many game companies have recognized the speed of users' content consumption as a big problem. As information is shared through the Web freely, users no longer have to go through monotonous trial and error processes to conquer the game. For example, in the case of Blizzard's Diablo 3, the provider was initially confident that it would take at least six months to finish the game. However, the normal level of the game was cleared by a Korean user in merely 6 hours of release, and the know-how of this gamer was instantly shared around the world via a YouTube channel. It is one of the most frequently cited story showing how difficult it is for game companies to control the game's overall lifespan. In this regard, cheating that promotes content consumption has the potential to pose a serious threat to game life and turnover. Nonetheless, in the case of the game of interest in this paper, the side effect is

unlikely to appear because the purpose of the game design is to consume the user's time. In other words, the game is created to provide ever-ending, yet extremely repetitive, contents. Thus the lifespan of the game does not decrease, even with multiboxing and bots.

By performing the granger causality test, I showed that the behavior of cheating users does not affect the playtime and purchase of other users. However, I do not see these results providing valuable insights to the real business. In other words, I think that the result of granger causality test could only be applied to some specific situations. I suspect that cheating did not affect other normal users since the number of cheaters is minimal. However, I am not entirely convinced that even if the number of cheaters increases, similar patterns will arise. In such respect, if I analyze the users who often encounter cheaters, the result may be different from the one explained in this study. Moreover, the unique characteristics of this game may also be the reason. Since this game has been in service for a long time, it could be said that only loyal users still remain playing. These loyal users may be dissatisfied with illegal cheating by cheating users, but they do not seem to drop out of the game or reduce their purchases.

From a platform standpoint, cheating can have a negative impact on the game. According to the previous studies, it seems obvious that cheating in online games is harmful to other normal users (Thawonmas et al., 2008; Gianvecchio et al., 2009; Yan and Randell, 2009; Kang et al., 2013). Even the existing studies claiming that cheating has a positive aspect to improve the game experience also agree that cheating has negative aspects to other normal users (references). Also, multiboxing and bots significantly increase traffic costs and server operating costs. In our results,

only 0.25% of the cheaters account for 6% of the total traffic, which shows that cheaters substantially increase the provider's operating costs. As mentioned in the introduction, such trend can be reinforced by everlasting arms race between users. Consequently, considering the sustainable operation of the game platform, it could be a better choice to ban the cheaters.

However, I was not also entirely in favor of a policy to ban cheating right away. I have already found that a small number of cheating users account for 12% of sales. For the provider, it is not easy to make a decision to ban users with such great importance. In the case of Free to Play (F2P) game discussed in this paper, a few hardcore users are highly salient. According to Swrve (2014), over 60% of mobile F2P game revenues are from just 0.13% of loyal users. Our case is no exception; only 1.8% of users (1,500 users) account for 70% of total sales. Under the circumstances, it could be unwise to easily give up 0.25% of cheating users (207 users).

In the end, I had to think of new alternatives to solve this problem, while minimizing the risk of losing highly valued users. To that end, I decided to focus more on behavioral motivations of cheaters. By closely observing the behavior of the 207 cheating users, I concluded that the outdated game designs that force users to engage in menial and repetitive activities is the primary cause of cheating. Cheaters were bored to spend too much time to grow their avatars and wanted to reduce tedious iterations by cheating. Based on such insights, I advised the provider that the direction of the new update should focus on reducing the advantage of cheating and increasing the velocity of the game playing and the

variety of contents. As a result, after the new update reflecting our advice, the revenue has once again turned upward.

There have been cases in which commercial successes have been achieved in game domain by focusing on the causes of cheating and solving them. A good example is a case in which a bot is installed as a basic user interface in mobile MMORPG games. In the early days of smartphones, puzzles and casual games were the mainstream due to technical limitations of mobile devices. As the performance of smart phones has improved dramatically, MMORPGs that were generally enjoyed on PCs are becoming more and more prevalent on mobile networks. However, unlike PCs that use a mouse and a keyboard, the mobile environment, which requires the use of touch screens and fingers, was not entirely suitable for MMORPG games. Hence, users became tired of playing mobile MMORPGs, and as a result, many users started to use bots to play automatically. In response, some companies have succeeded in using bots as their default user interface for their games rather than forbidding them. As a result, most of the mobile MMORPGs currently have automatic playing mode as a basic function, and many users enjoy such characteristics, though quite different from those of PC MMORPGs.

There is a comparable case for hacking that users manipulate the game data directly: a mod (short for "modification"). A mod is an alteration that modifies some aspect of a game, such as how it behaves or looks. Mods may reach from small modifications to complete overhauls, and they can enhance the value and interest of the game (Mod (video gaming), n.d.). In the early days, mod was also considered a kind of cheating that negatively affects the game. But now mods have arguably turned into an increasingly important factor in the success of certain

games, as they add desirable qualities to the original work (Postigo, 2007). For this reason, many major game developers, such as Valve Corporation, id Software and Bethesda, provide making tools and documentations to support mod makers. This case could be also seen as an instantiation of the “wisdom of crowd” (Surowiecki, 2005).

It is not so easy to decide whether or not to allow cheating activities in the game. As discussed in this paper, cheating is complicated by the trade-off between various pros and cons, and the overall effect of cheating can vary depending on the game design and the environment surrounding it. Therefore, in order to make decisions about cheating, it is absolutely necessary to understand the phenomenon accurately by analyzing each argument. Based on the results of the analysis, it is desirable to establish strategies to minimize the disadvantages of cheating while taking the advantages of cheating as in cases of mods, bots in mobile MMORPGs. You cannot have your cake and eat it too, but you can eat some pieces of your cake and keep other pieces.

The research on cheating in online games still has many areas to be studied. The game industry is huge enough to exceed the revenue of \$100 billion worldwide by 2017. Especially, mobile games play an important role, accounting for 42% (\$46.1 billion) of the market. Despite the importance of the mobile game market, there is not much literature regarding cheating in mobile game environment, particularly for quantitative research using secondary data. This can be good research topics in the future because cheating in mobile games is completely different from cheating in the PC-based online games I have covered in this paper. Mobile online games have similar characteristics to single-player games due to the limitations in the

screen size and device performance. In other words, unlike PC-based online games in which a large number of users interact simultaneously on a screen, a single user enjoys the game alone and then the record of the game is in cooperation with that of other users. Otherwise, the user can engage in competition with only a handful of users, after they play alone for a while. As a result, two negative effects that can occur when cheating occurs in online games can be somewhat mitigated in mobile games. First, in mobile games, it is difficult for other users to observe play directly. Therefore, even if there is a cheater, the cheater may be relatively less deprived of the other users. Second, due to the characteristics of mobile games, which have relatively few communications between the server and the device, the cost of traffic increases due to bots and multiboxing users is relatively smaller than that of PC game. This is one of the reasons why many mobile games have been able to adopt bots as a basic user interface.

Another interesting future research topic could be about the cheating behaviors related with gold farming and game sweatshop. These phenomena have taken place since the rapid expansion of the economy surrounding online games. Gold farming refers to the activity of playing a multiplayer online game to obtain in-game currency (Heeks, 2008). Generally, rich users from developed countries, willing to save their hours of playing time, pay to a company who hire gold farmers from developing countries (Barboza, 2005; see Fig 10). Such company is referred to as sweatshops since the gold farmers are generally paid very low wages (Jin, 2006). These companies also provide a service called “power leveling” that generate high-level avatars on behalf of clients (Thompson, 2005).

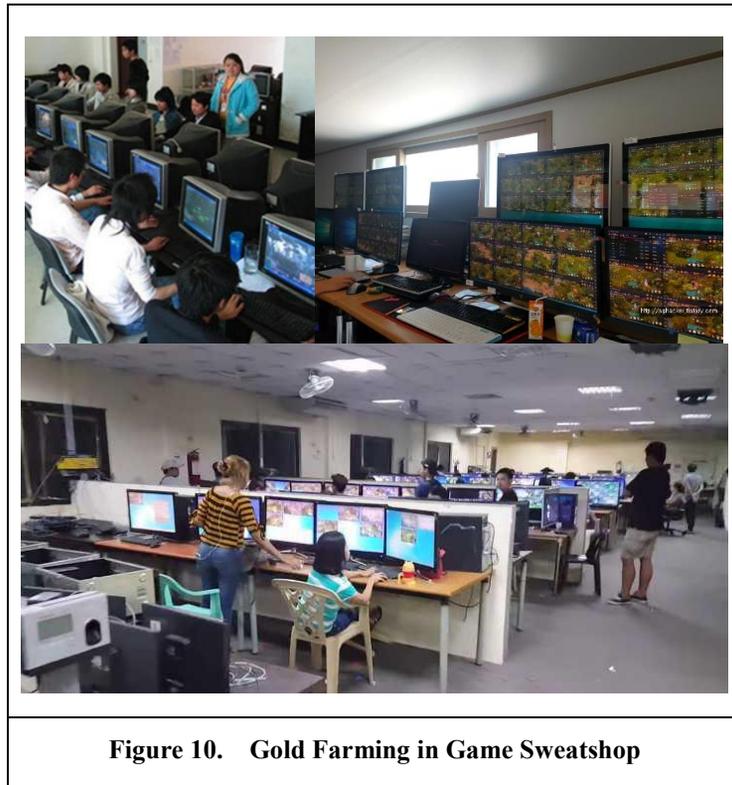


Figure 10. Gold Farming in Game Sweatshop

As the gold farming and power leveling through sweatshop became popular, overall cheating trend has changed greatly. Sweatshop usually operates 24 hours a day, 7 days a week and makes workers to play games at least 10 hours a day, taking advantage of relatively low labor costs (Thompson, 2005). In this case, the effect is the same as cheating, but it can be free from security solutions that detect bots based on behavior patterns. It is also very difficult to identify this type of cheating if the playtime per account is adjusted appropriately.

The empirical research on how the presence of sweatshops affects the gaming platform could also be an interesting and meaningful study. Many game companies in the field are aware of the existence of sweatshops, but they are not sure if it is the right decision to ban them. In the game industry, there is a view that the size of

illegal ecosystems, such as workshops and Real Money Trading (RMT), is a signal that shows how valuable the game is. In the case of RMT, there are previous studies that assert that RMT increases the demand for games (Jung et al., 2011) and plays an important role in the commercial success of games (Huhh, 2006). I often hear from many game industry people that their customers, who have very high value, do not stay in the game for long time unless the illegal ecosystem continues. Whether the existence of sweatshops has a positive impact on ecosystems, such as the case of RMT, or whether industry people are wrong, would be a very valuable research direction to draw conclusions based on data analysis.

In this study, I identified multiboxing cheaters and measured their impacts. In addition, I addressed the data availability issues such as unlabeled training set and lack of data, and proposed a method to overcome such pitfalls in data analysis. I chose a rule-based method and exploited various techniques of time series analysis and string processing algorithms. Our method also succeeds in avoiding large-scale transaction processing or complex development process, which are quite common in the existing cheating detection methods.

I believe that our paper gives useful business implications to policymakers and game industry managers informing the impact of hacking tools on sales and users' behavior. With respect to theoretical contribution, there is little rigorous research to analyze whether, and how much, online game cheating affects firms' sales and users' behavior. Especially, there exists scant research regarding multi-boxing behaviors, even though such behaviors are increasing due to recent surge in computing power among users. In such context, our study contributes to academic literature regarding impacts of cheating behaviors in online games.

Our study has several limitations. In order to verify the accuracy of the results, I used a heuristic method for a game operator to observe users identified as cheating users. Despite a high percentage of users who I identified as cheaters were actually cheaters, I did not assure how many actual cheating users could be in the group who were not identified as cheating users. In other words, I confirm that the precision of our model is reliable, but I am not sure the level of recall. Although this is a fairly common problem for cases that examine unlabeled problems, our case is no exception. Another problem is that in the case of hardcore users who play close to 24 hours a day, I do not know if they are cheaters or not. The game provider considers these users as a cheater based on the fact that it is impossible for a person to play games without rest. Nevertheless, it is the limit of our study that our method could not capture such pattern. I believe that these limitations stem from the need to create an identification model with scarce data to overcome the data availability issue. If further research can solve those limitations in the future, it would be a well-grounded study about cheating in online game.

9. References

- Aboukhadijeh, F. (2009, June 2). Cheating in Video Games. Retrieved from <https://feross.org/cheating-in-video-games/>
- Adams, J. S. (1963). Towards an understanding of inequity. *The Journal of Abnormal and Social Psychology*, 67(5), 422.
- Adams, J. S. (1965). Inequity in social exchange. *Advances in experimental social psychology*, 2, 267-299.
- Ahmad, M. A., Keegan, B., Srivastava, J., Williams, D., and Contractor, N. 2009. "Mining for Gold Farmers: Automatic Detection of Deviant Players in Mmogs," *Computational Science and Engineering*, 2009. CSE'09. International Conference on: IEEE, pp. 340-345.
- Arora, A., Telang, R., and Xu, H. 2008. "Optimal Policy for Software Vulnerability Disclosure," *Management Science* (54:4), pp. 642-656.
- Ashenfelter, O. C., & Card, D. (1984). Using the longitudinal structure of earnings to estimate the effect of training programs.
- August, T., and Tunca, T. I. 2008. "Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions," *Information Systems Research* (19:1), pp. 48-70.
- Barboza, D. (2005, December 9). Ogre to Slay? Outsource It to Chinese. *The New York Times*. Retrieved from

<http://www.nytimes.com/2005/12/09/technology/ogre-to-slay-outsourcer-it-to-chinese.html>

- Benkabou, S. E., Benabdeslem, K., & Canitia, B. (2017). Unsupervised outlier detection for time series by entropy and dynamic time warping. *Knowledge and Information Systems*, 1-24.
- Berndt, D. J., and Clifford, J. 1994. "Using Dynamic Time Warping to Find Patterns in Time Series," *KDD workshop: Seattle, WA*, pp. 359-370.
- Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M., & Iamnitchi, A. (2014). Cheating in online games: A social network perspective. *ACM Transactions on Internet Technology (TOIT)*, 13(3), 9.
- Boulnemour, I., Boucheham, B., & Benloucif, S. (2016, April). Improved Dynamic Time Warping for Abnormality Detection in ECG Time Series. In *International Conference on Bioinformatics and Biomedical Engineering* (pp. 242-253). Springer, Cham.
- Bounie, D., Bourreau, M., and Waelbroeck, P. 2006. "Piracy and Demands for Films: Analysis of Piracy Behavior in French Universities,").
- Brizan, D. G., & Tansel, A. U. (2006). A survey of entity resolution and record linkage methodologies. *Communications of the IIMA*, 6(3), 5.
- Carvalho, L. F., Rodrigues, J. J., Barbon, S., & Proenca, M. L. (2013, September). Using ant colony optimization metaheuristic and dynamic time warping for anomaly detection. In *Software, Telecommunications and Computer*

Networks (SoftCOM), 2013 21st International Conference on (pp. 1-5).
IEEE.

Chen, K. T., & Hong, L. W. (2007, September). User identification based on game-play activity patterns. In Proceedings of the 6th ACM SIGCOMM workshop on Network and system support for games (pp. 7-12). ACM.

Chen, K. T., Pao, H. K. K., & Chang, H. C. (2008, October). Game bot identification based on manifold learning. In Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games (pp. 21-26). ACM.

Chen, K. T., Jiang, J. W., Huang, P., Chu, H. H., Lei, C. L., & Chen, W. C. (2008). Identifying MMORPG bots: A traffic analysis approach. EURASIP Journal on Advances in Signal Processing, 2009(1), 797159.

Chen, V. H. H., & Wu, Y. (2015). Group identification as a mediator of the effect of players' anonymity on cheating in online games. Behaviour & Information Technology, 34(7), 658-667.

Consalvo, M. (2006, December 14). Cheating is good for you. Forbes. Retrieved from https://www.forbes.com/2006/12/10/video-games-cheating-tech-cz_mc_games06_1212consalvo.html

Consalvo, M. (2009). Cheating: Gaining advantage in videogames. Mit Press.

Cox, K. C., Eick, S. G., Wills, G. J., and Brachman, R. J. 1997. "Brief Application Description; Visual Data Mining: Recognizing Telephone Calling Fraud," Data Mining and Knowledge Discovery (1:2), pp. 225-231.

- Dehejia, R. H., and Wahba, S. 2002. "Propensity Score-Matching Methods for Nonexperimental Causal Studies," *Review of Economics and statistics* (84:1), pp. 151-161.
- Difference in differences. (n.d.). In Wikipedia. Retrieved May 4, 2017, from https://en.wikipedia.org/wiki/Difference_in_differences
- Drachen, A., Lundquist, E. T., Kung, Y., Rao, P., Klabjan, D., Sifa, R., & Runge, J. (2016). Rapid Prediction of Player Retention in Free-to-Play Mobile Games. arXiv preprint arXiv:1607.03202.
- Duh, H. B. L., & Chen, V. H. H. (2009, July). Cheating behaviors in online gaming. In *International Conference on Online Communities and Social Computing* (pp. 567-573). Springer, Berlin, Heidelberg.
- Ejsing-Duun, S., Hanghoj, T., & Karoff, H. S. (2013, January). Cheating and Creativity in Pervasive Games in Learning Contexts. In *European Conference on Games Based Learning* (p. 149). Academic Conferences International Limited.
- Ferretti, S. 2008. "Cheating Detection through Game Time Modeling: A Better Way to Avoid Time Cheats in P2p Mogs?," *Multimedia tools and applications* (37:3), pp. 339-363.
- Gal-Oz, A., and Zuckerman, O. 2015. "Embracing Cheating in Gamified Fitness Applications," *Proceedings of the 2015 Annual Symposium on Computer-Human Interaction in Play: ACM*, pp. 535-540.

- Gianvecchio, S., Wu, Z., Xie, M., and Wang, H. 2009. "Battle of Botcraft: Fighting Bots in Online Games with Human Observational Proofs," Proceedings of the 16th ACM conference on Computer and communications security: ACM, pp. 256-268.
- Gino, F., & Wiltermuth, S. S. (2014). Evil genius? How dishonesty can lead to greater creativity. *Psychological science*, 25(4), 973-981.
- Goga, O. (2014). Matching user accounts across online social networks: methods and applications (Doctoral dissertation, LIP6-Laboratoire d'Informatique de Paris 6).
- Golle, P., and Ducheneaut, N. 2005. "Preventing Bots from Playing Online Games," *Computers in Entertainment (CIE)* (3:3), pp. 3-3.
- Green, G., & Kaufman, J. C. (2015). *Video Games and Creativity*. Academic Press.
- Greene, W. H. (2007). *Econometric analysis*. Pearson Education.
- Greenland, S., Mansournia, M. A., & Altman, D. G. (2016). Sparse data bias: a problem hiding in plain sight. *bmj*, 352, i1981.
- Hadji, F., Sifa, R., Drachen, A., Thureau, C., Kersting, K., & Bauckhage, C. (2014, August). Predicting player churn in the wild. In *Computational intelligence and games (CIG)*, 2014 IEEE conference on (pp. 1-8). IEEE.
- Heeks, R. (2008). Current analysis and future research agenda on "Gold Farming": Real-world production in developing countries for the virtual economies of

online games. Institute for Development Policy and Management, University of Manchester.

Hilaire, S., Kim, H. C., & Kim, C. K. (2010, June). How to deal with bot scum in MMORPGs?. In Communications Quality and Reliability (CQR), 2010 IEEE International Workshop Technical Committee on (pp. 1-6). IEEE.

Hennig-Thurau, T., Henning, V., and Sattler, H. 2007. "Consumer File Sharing of Motion Pictures," *Journal of Marketing* (71:4), pp. 1-18.

Huhh, J. S. (2006). Effects of real-money trading on MMOG demand: A network externality based explanation.

Imbens, G., & Wooldridge, J. (2007). Difference-in-differences estimation. National Bureau of Economics Research Working Paper.

Izakian, H., Pedrycz, W., & Jamal, I. (2015). Fuzzy clustering of time series data using dynamic time warping distance. *Engineering Applications of Artificial Intelligence*, 39, 235-244.

Jeng, A. B., and Lee, C. L. 2013. "A Study on Online Game Cheating and the Effective Defense," *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*: Springer, pp. 518-527.

Jin, G. (2006). Chinese gold farmers in the game world. *Consumers, Commodities & Consumption*, 7(2), 7-2.

Jung, G., Lee, B., Yoo, B., & Brynjolfsson, E. (2011). Analysis of the relationship between virtual goods trading and performance of virtual worlds.

- Kang, A. R., Woo, J., Park, J., & Kim, H. K. (2013). Online game bot detection based on party-play log analysis. *Computers & Mathematics with Applications*, 65(9), 1384-1395.
- Keogh, E., and Ratanamahatana, C. A. 2005. "Exact Indexing of Dynamic Time Warping," *Knowledge and information systems* (7:3), pp. 358-386.
- Kim, H., Hong, S., and Kim, J. 2005. "Detection of Auto Programs for Mmorpgs," *Australasian Joint Conference on Artificial Intelligence*: Springer, pp. 1281-1284.
- Kirman, B., Lineham, C., and Lawson, S. 2012. "Exploring Mischief and Mayhem in Social Computing Or: How We Learned to Stop Worrying and Love the Trolls," *CHI'12 Extended Abstracts on Human Factors in Computing Systems*: ACM, pp. 121-130.
- Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. In *Networking, sensing and control, 2004 IEEE international conference on* (Vol. 2, pp. 749-754). IEEE.
- Larsen, Kim. 2016. "Making Causal Impact Analysis Easy", <http://multithreaded.stitchfix.com/blog/2016/01/13/market-watch/>
- Lechner, M. 2011. *The Estimation of Causal Effects by Difference-in-Difference Methods*. Now.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
- Mitterhofer, S., Kruegel, C., Kirda, E., and Platzer, C. 2009.

"Server-Side Bot Detection in Massively Multiplayer Online Games," IEEE Security & Privacy (7:3).

Lee, D. (2017). Anomaly Detection in Multivariate Non-stationary Time Series for Automatic DBMS Diagnosis. arXiv preprint arXiv:1708.02635.

Li, G., Yuan, T., Qin, S. J., and Chai, T. 2015. "Dynamic Time Warping Based Causality Analysis for Root-Cause Diagnosis of Nonstationary Fault Processes," IFAC-PapersOnLine (48:8), pp. 1288-1293.

Ma, L., Montgomery, A., Singh, P., and Smith, M. D. 2011. "Pre-Release Movie Piracy and Box Office Sales: Estimates and Policy Implications." Citeseer.

Mahlmann, T., Drachen, A., Togelius, J., Canossa, A., & Yannakakis, G. N. (2010, August). Predicting player behavior in tomb raider: Underworld. In Computational Intelligence and Games (CIG), 2010 IEEE Symposium on (pp. 178-185). IEEE.

Malhotra, A., Totti, L., Meira Jr, W., Kumaraguru, P., & Almeida, V. (2012, August). Studying user footprints in different online social networks. In Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on (pp. 1065-1070). IEEE.

Mod (video gaming). (n.d.). In Wikipedia. Retrieved October 9, 2017, from [https://en.wikipedia.org/wiki/Mod_\(video_gaming\)](https://en.wikipedia.org/wiki/Mod_(video_gaming))

Mönch, C., Grimen, G., and Midtstraum, R. 2006. "Protecting Online Games against Cheating," Proceedings of 5th ACM SIGCOMM workshop on Network and system support for games: ACM, p. 20.

- Phua, C., Lee, V., Smith, K., and Gayler, R. 2010. "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," arXiv preprint arXiv:1009.6119).
- Postigo, H. (2007). Of mods and modders: Chasing down the value of fan-based digital game modifications. *Games and Culture*, 2(4), 300-313.
- Pritchard, M. 2000. "How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It," *Gamasutra*, July (24).
- Quasi-experiment. (n.d.). In Wikipedia. Retrieved May 4, 2017, from <https://en.wikipedia.org/wiki/Quasi-experiment>
- Ridley, M. (1994). *The red queen: Sex and the evolution of human nature*. Penguin UK.
- Rob, R., and Waldfogel, J. 2007. "Piracy on the Silver Screen," *The Journal of Industrial Economics* (55:3), pp. 379-395.
- Rossignol, J. (2009, November 28). Cheating in games: the good, the bad, and the entirely necessary. *Techradar*. Retrieved from <http://www.techradar.com/news/gaming/cheating-in-games-the-good-the-bad-and-the-entirely-necessary-653045>
- Salvador, S. W. (2004). Learning states for detecting anomalies in time series.
- Schmitt, E., Tull, C., & Atwater, P. (2017). Extending Bayesian structural time-series estimates of causal impact to many-household conservation initiatives. arXiv preprint arXiv:1708.02395. (DTW)

- Schwieren, C., & Weichselbaumer, D. (2010). Does competition enhance performance or cheating? A laboratory experiment. *Journal of Economic Psychology*, 31(3), 241-253.
- Sifa, R., Hadiji, F., Runge, J., Drachen, A., Kersting, K., & Bauckhage, C. (2015). Predicting purchase decisions in mobile free-to-play games. *Proc. of AAAI AIIDE*.
- Smith, A. (1827). *An Inquiry into the Nature and Causes of the Wealth of Nations* (No. 25202). Printed at the University Press for T. Nelson and P. Brown.
- Smith, M. D., and Telang, R. 2009. "Competing with Free: The Impact of Movie Broadcasts on Dvd Sales and Internet Piracy 1," *mis Quarterly* (33:2), pp. 321-338.
- Surowiecki, J. (2005). *The wisdom of crowds*. Anchor.
- Swrve. (2014). *Mobile Games Monetization Report*. Swrve Inc.
- Swrve. (2016). *MONETIZATION REPORT 2016: Lifting the lid on player spend patterns in mobile*. San Francisco, CA: Swrve New Media Inc.
- Taylor, T. L. (2009). *Play between worlds: Exploring online game culture*. MIT Press.
- Thawonmas, R., Kurashige, M., and Chen, K.-T. 2007. "Detection of Landmarks for Clustering of Online-Game Players," *IJVR* (6:3), pp. 11-16.
- Thawonmas, R., Kashifuji, Y., and Chen, K.-T. 2008. "Detection of Mmorpg Bots Based on Behavior Analysis," *Proceedings of the 2008 International*

Conference on Advances in Computer Entertainment Technology: ACM, pp. 91-94.

Thompson, T. (2005). They play games for 10 hours—and earn£ 2.80 in a “virtual sweatshop.”. *The Observer*, 13.

Varvello, M., and Voelker, G. M. 2010. "Second Life: A Social Network of Humans and Bots," *Proceedings of the 20th international workshop on Network and operating systems support for digital audio and video: ACM*, pp. 9-14.

Van Kesteren, M., Langevoort, J., and Grootjen, F. 2009. "A Step in the Right Direction: Botdetection in Mmorpgs Using Movement Analysis," *Proc. of the 21st Belgian-Dutch Conference on Artificial Intelligence (BNAIC 2009)*, pp. 129-136.

Video game bot. (n.d.). In *Wikipedia*. Retrieved May 4, 2017, from https://en.wikipedia.org/wiki/Video_game_bot

Von Ahn, L., Blum, M., Hopper, N. J., and Langford, J. 2003. "Captcha: Using Hard Ai Problems for Security," *International Conference on the Theory and Applications of Cryptographic Techniques: Springer*, pp. 294-311.

Vy, N. D. K., & Anh, D. T. (2016, June). Detecting Variable Length Anomaly Patterns in Time Series Data. In *International Conference on Data Mining and Big Data* (pp. 279-287). Springer International Publishing.

Webb, S. D., & Soh, S. (2007, September). Cheating in networked computer games: a review. In *Proceedings of the 2nd international conference on Digital interactive media in entertainment and arts* (pp. 105-112). ACM.

- Winkler, W. E. 1990. "String Comparator Metrics and Enhanced Decision Rules in the Fellegi-Sunter Model of Record Linkage,").
- Yampolskiy, R. V., and Govindaraju, V. 2008. "Embedded Noninteractive Continuous Bot Detection," *Computers in Entertainment (CIE)* (5:4), p. 7.
- Yan, J. (2003, December). Security design in online games. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual* (pp. 286-295). IEEE.
- Yan, J., and Randell, B. 2005. "A Systematic Classification of Cheating in Online Games," *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games: ACM*, pp. 1-9.
- Yan, J. 2009. "Bot, Cyborg and Automated Turing Test (Transcript of Discussion)," *LECTURE NOTES IN COMPUTER SCIENCE* (1:5087), pp. 198-201.
- Yan, J., & Randell, B. (2009). An investigation of cheating in online games. *IEEE Security & Privacy*, 7(3).
- Yee, N. (2006). Motivations for play in online games. *CyberPsychology & behavior*, 9(6), 772-775.
- Yeung, S., Lui, J. C., Liu, J., and Yan, J. 2006. "Detecting Cheaters for Multiplayer Games: Theory, Design and Implementation," *Proc IEEE CCNC*, pp. 1178-1182.
- Yuan, T. 2014. *Process Data Analytics and Monitoring Based on Causality Analysis Techniques*. University of Southern California.

Zhong, Z. J. (2011). The effects of collective MMORPG (Massively Multiplayer Online Role-Playing Games) play on gamers' online and offline social capital. *Computers in human behavior*, 27(6), 2352-2363.

Essay 2

Churn Prediction in Mobile Casual Game

A Deep Sequence Classification Approach

1. Introduction

With expanding use of smartphones, the mobile game industry has become a tremendously pivotal business area. According to Takahashi (2016), mobile games generate about 85% of global mobile app market revenue in 2015. By 2020, the revenue of mobile game market is projected to reach \$74.6 billion. Hence, it could be contended with confidence that mobile game is now the biggest part of the mobile app content business (Milosevic et al., 2017).

With such trend, predicting customers' leaving in the mobile game market has become a more critical issue than ever. In general, retaining an existing customer costs several times less than acquiring a new customer (Castro and Tsuzuki, 2015). Moreover the cost of acquiring customers is rapidly increasing (Freier, 2015). If companies could know when and whether the customer will leave, they can significantly enhance customer retention and save high costs of recruiting new ones (Bin et al., 2007). Furthermore, with a well-functioning churn prediction model, companies can maximize profits by deploying aggressive marketing strategies targeted to customers that are likely to churn in the near future. For example, Tencent, one of the largest game service providers in China, developed a churn prediction model for targeted marketing. As a result of targeted push marketing, the rate of return has increased by utmost 326% compared to that of random push (Tencent Big Data, 2015).

Data preparation is one of the most challenging tasks in the big data environment (Jagadish et al., 2014). Data preparation comprises the process of gathering, cleaning, consolidating and structuring a data set (Henke et al., 2016). As the

volume and variety of data continue to grow, the costs of data preparation grow exponentially, both from a computing resource perspective and a labor-driven perspective (Haight, 2016). According to Press (2016), data preparation accounts for approximately 80% of the task of data scientists. Moreover, the dissemination of General-Purpose computing on Graphics Processing Units (GPGPU) significantly reduces the cost of model calculations, so data preparation becomes relatively a large part of big data analytics (Chen and Lin, 2014). Our task is not an exception; we use 50 parallel enterprise cloud servers for data preparation, but a single desktop computer with GTX 1080 Ti graphic card is sufficient for learning of prediction models. In this context, reducing the cost of data preparation is one of the most critical success factors in big data analytics (Jagadish et al., 2014).

In this study, I bring out a methodology to deal with churn prediction that fulfills two cardinal objectives. First, to minimize the cost of preparing the data for analysis. Second, to propose an algorithm that shows performance comparable to the performance of the existing algorithms. I succeed in significantly reducing the burden of the data preparation process by utilizing the sequence structure of the original log data. Besides, our sequence classification model based on CNN-LSTM outperforms the models of previous studies.

There are not many studies using deep learning as the main methodology in the IS field. According to Van Aken (2004), the main goal of design science research is to develop knowledge that the professionals of the discipline in question can use to design solutions for their field problems. Statistical learning theories have served as a useful kernel theory in achieving the goals of design science research (DSR). In particular, deep learning (which is one of state-of-the-art statistical learning

techniques) is expected to make many contributions in the future, in aspect of problem relevance, research contribution and design as a search process which is a part of the seven guidelines for DSR that Hevner et al. (2004) suggest. In this context, this study contribute to the growing area of design science research by constructing a deep learning model as an artifact which solve important business problem regarding prediction user's churn.

2. Definition of Churn

I define a user to have churned if he or she has played the game under 5 times within 2 weeks from the latest active week. A time span of seven days, Monday through Sunday, is declared as one week. Active week is a week in which there is at least one game play.

The definition of churn varies depending on the characteristic of the game and the purpose of the analytics (Castro and Tsuzuki, 2015). I borrow the definition of churn used by Runge et al. (2014) and Milošević et al. (2017). However, I modify 'last active day' to 'last active week' because defining churn on a weekly basis significantly reduces the burden of data preparation. I also take into account the predilections of game companies in which decisions are made on a weekly basis. The reason for defining a user who plays less than 5 times in 2 weeks as a churn user is considering the problem relevance aspect. According to the opinion of the game company, the user having the play count of 0 times within 2 weeks is likely to have already deleted the app or otherwise, it is extremely difficult to make the user interested in the game again through marketing. Hence, we set up the

definition of churn to play less than five times within 2 weeks to perform marketing before it is too late.

3. Related Works

Churn prediction has been studied in various fields such as customer relationship management, banking, telecommunication, social networks, and insurance (Ballings & Van Den Poel, 2012; Gür Ali & Aritürk, 2014; Dierkes, Bichler, & Krishnan, 2011; Ngonmang, Viennet, & Tchunte, 2012; Risselada, Verhoef, & Bijmolt, 2010).

In the game industry, research on churn prediction has also been actively pursued. These studies focus mainly on selecting important features for predicting user churn and attempting to predict user churn using a binary classification approach (Hadiji et al., 2014; Runge et al., 2014; Rothenbuehler et al., 2015).

With respect to methodology, diverse machine learning algorithms are frequently utilized to predict churn in various settings. More specifically, many studies build models using algorithms such as logistics regression, decision tree, support vector machine (SVM), random forest, gradient boosting, and neural networks (Runge et al., 2014; Hadiji et al., 2014; Gür Ali and Aritürk, 2014).

Runge et al. (2014) investigate a churn prediction study for high-value users in online casual games. They predicted churn for top 10% of high spending players of two free-to-play (F2P) mobile casual games using various algorithms (neural network, logistic regression, decision tree, and SVM). The performance of the results was evaluated using ROC_AUC. Kawale et al. (2009) investigate churn in

the MMORPG using social network analysis based on social influence among users. Nozhnin (2012) focuses on the first few minutes of gameplay. Hadiji et al. (2014) identify a various behavioral features useful for a churn prediction.

4. Data

In this study, I analyze a highly popular mobile casual game in Korea. The game was released in 2013 and ranked as first in 10 countries including Korea, Japan, Taiwan, and Thailand. Furthermore, the game has cumulative download counts of over 70 million.

I use data regarding the service in Korea, which are accumulated for four weeks from October 5, 2015 to November 1, 2015. The number of Monthly Active Users (MAUs) is about 3 million. Among them, about 1 million users have accessed in a week. The database consists of 73 tables and about 27,000 variables, most of which are stored in a log format with corresponding time stamps. The amount of data is about 120 GB per day, and consequently, a large-scale data set of 3.5 TB for a month is manipulated for analyses.

5. Method

5.1. Data Preparation

5.1.1. Sequence Process

We perform two kinds of methods, namely process A and process B, for data preparation and compare their corresponding results. A database engineer who has participated in the development of the game is in charge of this task.

In process A, I try to aggregate data scattered in many relational tables into one table using SQL join syntax. This is by far the most common way to prepare data for analysis (Ordonez, 2011). Table 1 exhibits a part of a resultant data set, which is manipulated through process A.

However, to extract the variables needed for the analysis through process A, I have to use complex join syntax (e.g. window or recursive queries) that leads to a heavy load on the servers. As a result, I am just able to extract only 25 variables that require only simple computations, even with 200 enterprise-level cloud servers. Also, it should be noted that a lot of labor costs are involved in creating queries. Hence, I attempt to overcome such impediments in process B.

Table 1. Part of the resultant data set from process A						
User ID	Week	Play Count	Purchase Count	Message Send	...	Churn
...
30617	1	37	4	57	...	0
30617	2	25	2	32	...	0
30617	3	12	0	14	...	1
...
1061731	1	23	3	19	...	0
1061731	2	54	7	82	...	0
...

In process B, we convert the log data in the database into the sequential format. First, I select about 78 variables that are deemed to be useful in predicting churn by referring to prior works and advice from domain experts. Then, I numbered each selected variable from 2 to 79 and converted each user's log data into a sequence of numbers. An integer '1' is assigned to a milestone which divides the user's sequence into 1 hour units. For example, if a user logs in, plays a game twice, earns a reward in the game, and receives a message from a friend, it can be represented as a sequence of integers '2, 13, 13, 7, 6' (see Figure 1). Since the log data stored in the database are in a time-based sequential format, as shown at the top of Figure 1, I am able to handle this process with simple SQL queries that require much less computing power than consumed in process A. Table 2 is a part of a resultant data set, which is manipulated through process B.

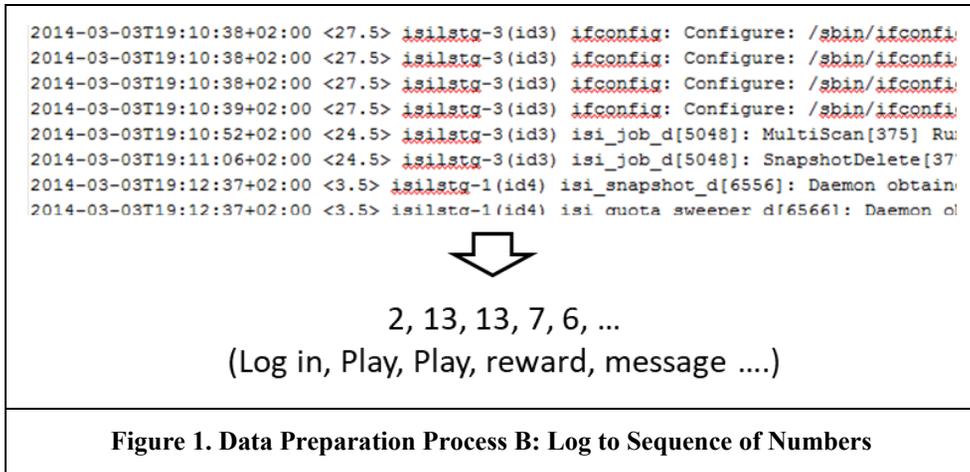


Table 2. Part of the resultant data set from process B			
User ID	Week	Sequence of Behaviors	Churn
...
30617	1	4,16,24,2,7,1,1,3,6,3,2...	0
30617	2	2,8,7,13,4,2,4,2,1,2,5,7...	0
30617	3	3,8,7,1,1,1,1,1,1,1,1...	1
...

I decide to use the sequence data from process B as an input to our churn prediction model. Through process B, I am able to extract better quality data while using only about 1/15 of the resources used in process A (see Table 3). If the quality of the information and the labor of writing highly complex queries are taken into consideration, such difference would be even more obvious.

5.1.2. Milestone

I introduce the concept of milestone to incorporate more information in the user's behavioral sequence. To put it more precisely, I insert an integer '1' in the user's sequence every hour, which separates the user's behaviors in one-hour units. Milestones greatly increase the quality of the data used in the analysis with relatively a lower level of effort. Suppose that there are users A and B with an identical behavior sequence of '13, 13, 13, 13, 13, 13, 13, 13'. Without milestones, these two would be regarded as exhibiting the same behavioral patterns. However, after inserting milestones, the patterns of these two can be distinguished. For instance, user A could have a pattern of '1, 13, 13, 13, 13, 13, 13, 13, 13, 1' while user B having '1, 13, 13, 1, 1, 1, 1, 13, 1, 1, 1, 1, 1, 13, 1, 1, 13, 1.' The two patterns

consist of the same sequence of behaviors, however, they have a completely different immersion. As a result, the two users' behavioral traits can be interpreted as rather different; the former is a heavy user who plays the game eight times in an hour, while the latter is a light user who plays the game one or two times every few hours.

The time distance between two adjacent milestones is commonly set to one hour since I consider an inherent limitation of LSTMs regarding the long-term dependency. In other words, LSTMs have the higher capacity to store information regarding previous states' compared to simple recurrent neural networks, but oftentimes such information, i.e., signals or memories, vanish in excessively lengthy sequences.

Without loss of generality, it could be asserted that if one sets the time distance between milestones smaller, the possibility of losing information grows larger, even though more information could be allowed for. The time distance of one hour between two neighboring milestones is the result of meticulously considering such trade-off between the richness of information and the probability of deteriorating long-term dependency.

Table 3. Details of Data Preparation Processes					
Process	Spec of Servers	# of Servers	# of Variables	Labor Time	Operation Time
Process A	AWS r3.2xlarge	200	25	High	7 hours
Process B	AWS r3.2xlarge	48	78	Low	2 hours

5.2. Prediction Model

I define the problem of predicting users' churn as a binary sequence classification problem (Graves, 2012). In more detail, I use the LSTM model of many to one structure, which takes each user's weekly log sequences regarding his or her behaviors as inputs and classifies each user as a churn or a stay over the next two weeks.

In addition, to improve the performance of the model and reduce computing cost, I employ Convolutional Neural Networks (CNN) along with a Long Short-Term Memory (LSTM) model. Moreover, recently developed techniques to ameliorate training of neural networks, including Batch Normalization, Embedding, Leaky ReLU, Spatial Dropout and Adam Optimizer, are utilized.

Figure 2 shows the details of the model. To start with, I set the length of the input sequence to 500. Sequences with more than 500 behaviors are pre-truncated, and sequences with less than 500 behaviors are pre-padded with zeros. Then, the data set is shuffled and divided into training set and test set by the ratio of 7:3. I also embed the user's 78 behaviors into a real valued vector with 64 elements. In an embedded vector, similar behaviors have rather smaller euclidean distance than the ones that are dissimilar from each other. This embedding layer reduces the complexity of the network (Dai and Le, 2015).

Before and after the convolution layer, I add batch normalization layers, which accelerate the training of deep networks by reducing internal covariate shift (Ioffe and Szegedy, 2015). The CNN layer is located prior to the LSTM layer and reduces the variance in frequency of the input (Tara et al., 2015). According to Sainath et al.

(2015), combining CNN and LSTM provides slight improvements over using LSTM only. As an activation function of the CNN layer, I use leaky rectified linear unit (Leaky ReLU). According to Xu et al. (2015), leaky ReLU could consistently improve the results by preventing dying ReLU problems in which ReLU neurons become inactive with any given input. After applying the activation function, a spatial dropout layer is attached to prevent overfitting. Finally, LSTM and a fully connected layer take place and then the result is finally classified as churn or stay using the sigmoid function.

In order to determine the depth and structure of the model and to tune the hyperparameters, I iterate a number of experiments. To enhance the efficiency of experimenting, I also use a Grid Search method to automate a part of hyperparameter tuning process (Bergstra et al., 2011).

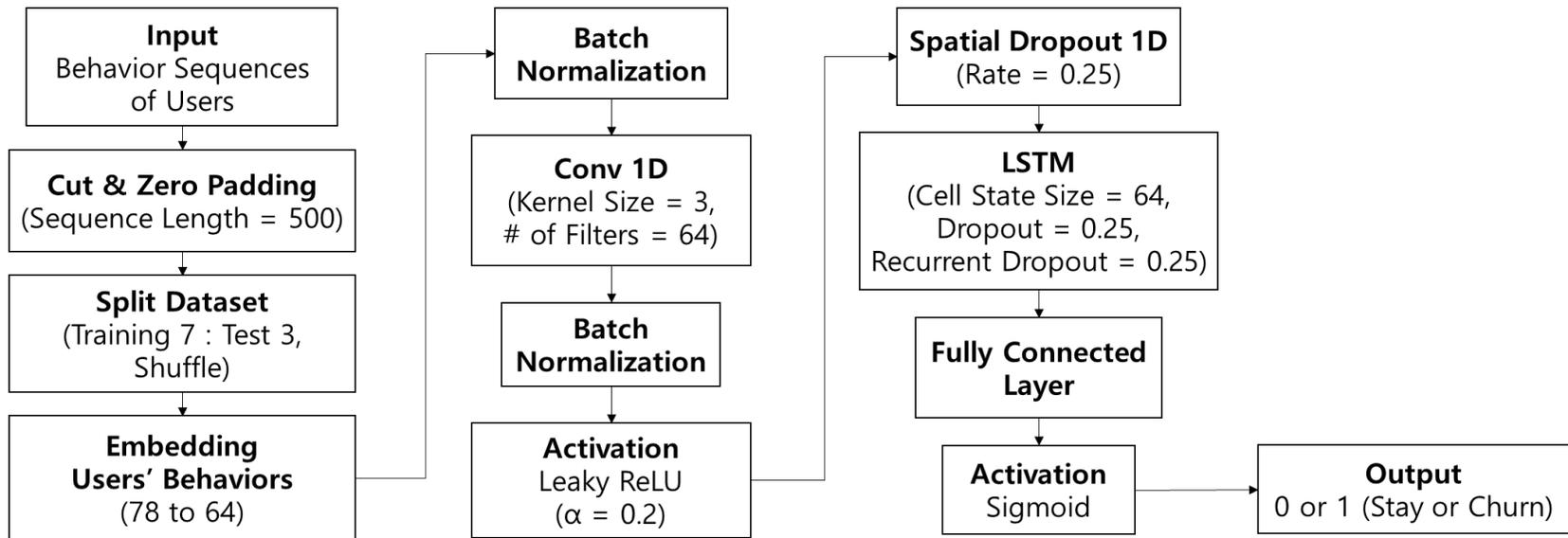


Figure 1. Details of Churn Prediction Model.

6. Result and Discussion

I use accuracy as a metric to evaluate the performance of the churn prediction model. The reason for using accuracy as the only metric is that our case does not suffer class imbalance problems. Many churn prediction studies suffer from class imbalance problems (Hadiji et al., 2014; Sifa et al., 2015). In such cases, the overall accuracy of the model tends to be overestimated. Assume that the distribution of class labels is highly skewed at a ratio of 9 to 1, positive and negative respectively. It is fairly easy to acquire 90% of accuracy by creating a model that classifies all the outputs as a positive class. Nevertheless, such model does not bear significant implications for business applications. Hence, it could be argued that considering accuracy as a sole indicator of a model's success is not recommendable. Considering ROC_AUC and f1-score at the same time can alleviate such problem (Burez and Poel, 2009; Jeni et al., 2013). However, in our case, churn and stay ratio is close to 1: 1 because we define a user to have churned if he or she has played the game under 5 times within 2 weeks from the latest active week. This means that it is enough to use an accuracy as a single evaluation metric. And we use ROC_AUC and f1-score only for comparison with other algorithms used in previous studies.

Table 4. Comparison with the results of other algorithms			
Model	Accuracy	ROC_AUC	F1-Score
Random Forest	77.1 %	0.7706	0.77
Extra Trees	77.4 %	0.7685	0.77
SVM	78.9 %	0.7840	0.79
Ada Boost	79.3 %	0.7876	0.79
Logistics Regression	79.4 %	0.7858	0.79
Gradient Boosted Model	80.1 %	0.7954	0.80
Deep Neural Network	80.5 %	0.8005	0.80
Our Model	81.1 %	0.8068	0.81

It could be concluded that our model shows better results to those of other models on all metrics. I suppose that the differences in data quality make the differences in the results. To reduce the cost of data preparation, I choose a sequence model that uses the structure of the log data as is. As a result, I am able to use 78 variables to train the churn prediction model, which are much more extensive than the variables used in previous studies. Our model also capacitates handling more information because it allows for each user's order, or sequence, of behaviors (Lipton et al., 2015). In other words, our approach based on LSTM can reflect not only the user's behaviors but also the context of the user's behaviors in the analysis.

Another advantage of our model is that it can be applied to any user playing the game. If I segment users into several groups, the performance of the model can be higher due to reduction in the intra-class variance (Fisher, 2015). However, the modeling and forecasting process can become complicated when user segmentations are taken into account. Hence, in order to increase the utility of

models in real-world business settings, I design a model without user segmentation, while not sacrificing a high level of performance. Therefore, it could be contended that our approach has a fairly valuable aspects from a real-world business perspective.

As the amount and variety of data increases, the cost of data preparation is ever increasing with an exponential rate. On the other hand, the widespread adoption of GPGPU dramatically reduces the cost of machine computation and leads to greater demand in larger quantity and higher quality data in the data analysis field. In light of such trend, our case is no exception, and the cost of data preparation is much greater than the cost of computational learning in models. Hence, it is becoming virtually mandatory to consider ways to reduce data preparation costs in predictive analysis. In this context, our proposed sequential approach, which uses the structure of log data as it is, is prospected to contribute to the growing academic literature on churn prediction. In particular, our model will be more useful in the game field that accumulates enormous amounts of log data.

There is a concern that LSTM has weaknesses in terms of computation compared to CNN or basic NN. However, I need to consider the whole process of data analysis, including data preprocessing. In the big data environment, there are many cases in which I need to spend a lot more resources on data preprocessing compared to those spent in model training. In addition, the emergence of the latest methodologies such as Simple Recurrent Unit (SRU), which increases the speed of sequential learning as much as CNN, shows the possibility of alleviating the computational weakness of LSTM (Lei and Zhang, 2017).

7. References

- Alan, RH, March, ST, Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly* , 28 (1), 75-105.
- Alex Graves. 2012. *Supervised sequence labelling with recurrent neural networks*. Springer.
- Ali, Ö. G., & Arıtürk, U. (2014). Dynamic churn prediction framework with more effective use of rare event data: The case of private banking. *Expert Systems with Applications*, 41(17), 7889-7903.
- Andrew M Dai and Quoc V Le. 2015. Semi-supervised sequence learning. in *Advances in Neural Information Processing Systems*, 3079-3087.
- Anne Freier. 2015. User acquisition cost for apps and games increases to \$3. Retrieved May 7, 2015 from <http://www.mobyaffiliates.com/blog/user-acquisition-costs-for-apps-and-games-increases-to-3/>
- Ballings, M., & Van den Poel, D. (2012). Customer event history for churn prediction: How long is long enough?. *Expert Systems with Applications*, 39(18), 13517-13522.
- Bing Xu, Naiyan Wang, Tianqi Chen and Mu Li. 2015. Empirical evaluation of rectified activations in convolutional network. arXiv preprint arXiv:1505.00853.
- Carlos Ordonez. 2011. Data set preprocessing and transformation in a database system. *Intelligent Data Analysis*, 15 (4). 613-631.

- Dierkes, T., Bichler, M., & Krishnan, R. (2011). Estimating the effect of word of mouth on churn and cross-buying in the mobile phone market with Markov logic networks. *Decision Support Systems*, 51(3), 361-371.
- D Takahashi. 2016. Mobile games hit \$34.8 B in 2015, taking 85% of all app revenues. Retrieved May, 28. 2016.
- Emiliano G Castro and Marcos SG Tsuzuki. 2015. Churn prediction in online games using players' login records: A frequency analysis approach. *IEEE Transactions on Computational Intelligence and AI in Games*, 7 (3). 255-265.
- Eunbyung Park. Groupout: A Way to Regularize Deep Convolutional Neural Network.
- Fabian Hadiji, Rafet Sifa, Anders Drachen, Christian Thureau, Kristian Kersting and Christian Bauckhage. 2014. Predicting player churn in the wild. in *Computational intelligence and games (CIG)*, 2014 IEEE conference on, IEEE, 1-8.
- G Press. 2016. Cleaning big data: Most time-consuming, least enjoyable data science task, survey says. *Forbes*, March, 23.
- Hadiji, F., Sifa, R., Drachen, A., Thureau, C., Kersting, K., & Bauckhage, C. (2014, August). Predicting player churn in the wild. In *Computational intelligence and games (CIG)*, 2014 IEEE conference on (pp. 1-8). IEEE.

- HV Jagadish, Johannes Gehrke, Alexandros Labrinidis, Yannis Papakonstantinou, Jignesh M Patel, Raghu Ramakrishnan and Cyrus Shahabi. 2014. Big data and its technical challenges. *Communications of the ACM*, 57 (7). 86-94.
- James Haight. 2016. Quantifying the Case for Enhanced Data Preparation. Retrieved February 26, 2016 from <http://bluehillresearch.com/quantifying-the-case-for-enhanced-data-preparation/>
- James S Bergstra, Rémi Bardenet, Yoshua Bengio and Balázs Kégl. 2011. Algorithms for hyper-parameter optimization. in *Advances in Neural Information Processing Systems*, 2546-2554.
- Jonathan Burez and Dirk Van den Poel. 2009. Handling class imbalance in customer churn prediction. *Expert Systems with Applications*, 36 (3). 4626-4636.
- Julian Runge, Peng Gao, Florent Garcin and Boi Faltings. 2014. Churn prediction for high-value players in casual social games. in *Computational Intelligence and Games (CIG), 2014 IEEE Conference on*, IEEE, 1-8.
- Kawale, J., Pal, A., & Srivastava, J. (2009, August). Churn prediction in MMORPGs: A social influence based approach. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 4, pp. 423-428). IEEE.
- László A Jeni, Jeffrey F Cohn and Fernando De La Torre. 2013. Facing imbalanced data--Recommendations for the use of performance metrics. in

Affective Computing and Intelligent Interaction (ACII), 2013 Humaine Association Conference on, IEEE, 245-251.

Luo Bin, Shao Peiji and Liu Juan. 2007. Customer churn prediction based on the decision tree in personal handyphone system service. in Service Systems and Service Management, 2007 International Conference on, IEEE, 1-5.

Miloš Milošević, Nenad Živić and Igor Andjelković. 2017. Early churn prediction with personalized targeting in mobile social games. Expert Systems with Applications, 83. 326-332.

Ngonmang, B., Viennet, E., & Tchuente, M. (2012, August). Churn prediction in a real online social network using local community analysis. In Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on (pp. 282-288). IEEE.

Nicolaus Henke, Jacques Bughin, Michael Chui, James Manyika, Tamim Saleh, Bill Wiseman and Guru Sethupathy. 2016. The age of analytics: Competing in a data-driven world. McKinsey Global Institute. 4.

Nozhnin, D. (2012). Predicting churn: Data-mining your game. Gamasutra. URL: http://www.gamasutra.com/view/feature/170472/predicting_churn_datamining_your_.php.

Rafet Sifa, Fabian Hadiji, Julian Runge, Anders Drachen, Kristian Kersting and Christian Bauckhage. 2015. Predicting purchase decisions in mobile free-to-play games. Proc. of AAAI AIIDE.

- Risselada, H., Verhoef, P. C., & Bijmolt, T. H. (2010). Staying power of churn prediction models. *Journal of Interactive Marketing*, 24(3), 198-208.
- Ronald Aylmer Fisher. 1992. Statistical methods for research workers. in *Breakthroughs in Statistics*, Springer, 66-70.
- Rothenbuehler, P., Runge, J., Garcin, F., & Faltings, B. (2015, November). Hidden markov models for churn prediction. In *SAI Intelligent Systems Conference (IntelliSys)*, 2015 (pp. 723-730). IEEE.
- Runge, J., Gao, P., Garcin, F., & Faltings, B. (2014, August). Churn prediction for high-value players in casual social games. In *Computational Intelligence and Games (CIG)*, 2014 IEEE Conference on (pp. 1-8). IEEE.
- Sergey Ioffe and Christian Szegedy. 2015. Batch normalization: Accelerating deep network training by reducing internal covariate shift. in *International Conference on Machine Learning*, 448-456.
- Seungwook Kim, Daeyoung Choi, Eunjung Lee and Wonjong Rhee. 2017. Churn prediction of mobile and online casual games using play log data. *PloS one*, 12 (7). e0180735.
- Tara N Sainath, Oriol Vinyals, Andrew Senior and Haşim Sak. 2015. Convolutional, long short-term memory, fully connected deep neural networks. in *Acoustics, Speech and Signal Processing (ICASSP)*, 2015 IEEE International Conference on, IEEE, 4580-4584.
- Tao Lei and Yu Zhang. 2017. Training RNNs as Fast as CNNs. *arXiv preprint arXiv:1709.02755*.

Tencent Big Data. 2015. Based on the Mobile Games platform Tencent pigeon churn prediction model overview. Retrieved June 12, 2015 from <http://prog3.com/article/2015-06-12/2824948>

Xue-Wen Chen and Xiaotong Lin. 2014. Big data deep learning: challenges and perspectives. IEEE access, 2. 514-525.

Zachary C Lipton, John Berkowitz and Charles Elkan. 2015. A critical review of recurrent neural networks for sequence learning. arXiv preprint arXiv:1506.00019.

국문 초록

온라인 게임에서 유저의 행태에 관한 연구

본 연구는 온라인 게임에서 유저의 행태에 관한 연구이며, 총 2개의 에세이로 구성되어 있다.

첫 번째 연구에서는, 멀티박싱으로 불리는 불법 사용자들을 찾아내고, 그들이 게임 플랫폼에 어떤 영향을 끼치는지 밝혀냈다. 이 과정에서 많은 게임 회사들이 겪고 있는 데이터 가용성 문제를 해결하기 위해 유저의 ID와 구매기록 그리고 플레이타임만을 이용해 분석을 수행하였다. 또한 기존의 불법 탐지 연구들에서 선행되어야 했던 복잡한 개발 과정이 필요없는 분석 프레임워크를 제시하고자 했다. 불법 사용자들을 구분하기 위해 본 연구에서는 DTW (Dynamic Time Warping)과 JWD (Jarow-Winkler distance) 알고리즘을 사용했다. 사용자의 불법 행위가 유저의 행태에 어떤 영향을 끼치는지 밝혀내기 위해서는 DID (Difference in Differences)를 이용한 Quasi-Experiment를 수행하였다. 결과적으로 전체 유저의 약 0.25% 정도의 소수의 유저들이 불법 행위를 저지르는 사용자로 판명되었다. 그러나 이들은 전체 매출의 약 12%를 차지할 정도로 중요성이 큰 사용자로 판명되었다. 또한 멀티박싱이라 불리는 불법 행위를 저지른 이후 사용자들의 플레이타임과 구매가 각각 102%, 79%씩 증가했다는 사실을 밝혀냈다. 또한 추가 분석을 통해 이러한 효과가 중장기적으로 지속된다는 점을 밝히고, 이런 불법 유저들의 행태가 다른 유저들의 구매와 플레이타임에 영향을 끼치지 않는다는 사실도 밝혀냈다.

두 번째 연구에서는 두 가지 목적을 갖고 온라인 게임에서의 유저들의 이탈을 예측하는 모형을 개발했다. 첫째, 빅데이터 환경에서 중요하게

떠오른 데이터 전처리 비용을 최소화한다. 둘째, 기존의 관련 분야에서 사용되던 모형들에 비해 더 나은 성능을 보인다. 이를 위해 시퀀스 데이터를 이용한 딥러닝 (LSTM) 기반의 모형을 제안했으며, 그 결과 본 연구에서 제안한 CNN-LSTM 기반의 모형은 데이터 전처리 비용을 대폭 감소시킬 뿐만 아니라 기존 모형들에 비해 더 나은 결과를 보였다.

주요어: 온라인게임, 데이터분석, 이상행동탐지, 멀티박싱, 이탈예측

학 번: 2014-30155